Math. Appl. **10** (2021), 103–113
DOI: 10.13164/ma.2021.09

ON CUBIC POLYNOMIALS WITH A GIVEN DISCRIMINANT

JIŘÍ KLAŠKA

Abstract. Let $D \in \mathbb{Z}$ and let C_D be the set of all monic cubic polynomials with integer coefficients and with the discriminant equal to D. In this paper we devise a method for determining the set C_D. Our method is closely related to integer solutions of Mordell's equation. A complete discussion of the case $D = 0$ is also included.

1. Introduction

In 1940, B. N. Delone and D. K. Faddeev [2, p. 313] posed the problem of giving an algorithm for finding all cubic monic polynomials with integer coefficients and a given non-zero discriminant. In this paper, we provide a solution to the problem closely related to Mordell's equation. In addition, a computer program based on our method yields results leading to new interesting questions.

Recall that the equation

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

is called Mordell's equation in honour of the contribution Louis Joel Mordell has made to this subject. In 1920 Mordell proved [18] that, for any given $0 \neq k \in \mathbb{Z}$, there are at most finitely many $X, Y \in \mathbb{Z}$ satisfying (1.1). Mordell's equation has had a long history. First discoveries concerning (1.1) were given in Dickson [3, pp. 533–539] going back to the work of Bachet of 1621. From the extensive literature concerning (1.1) see, for example, [1, 6–8] and, [17]. There is a standard method for computing all integer solutions of (1.1) using David's bounds and lattice reduction. This method can be found, for example, in [19]. At present, this method is implemented in several computer algebra packages, including Magma and Pari (Sage).

Let $D \in \mathbb{Z}$ and let

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

where

$$D_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

is the discriminant of $f(x)$. It is clear that the problem of determining all polynomials in C_D for a given $D \in \mathbb{Z}$ is equivalent to finding all integer solutions of the Diophantine equation $D_f = D$. In Section 3, we prove that, for any $0 \neq D \in \mathbb{Z}$,

MSC (2020): primary 11D25, 11D45, 11Y50.
Keywords: cubic polynomial, discriminant, Mordell's equation.
Dedicated to professor Ladislav Skula.

the equation $D_f = D$ can be reduced to Mordell's equation (1.1) with $k = -432D$. The exceptional case of $D = 0$ will be examined separately. Finally, throughout this paper, the following notation will be adopted. If A is a finite set, $\#A$ denotes the number of elements of A.

2. Equivalence on the set C_D.

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ and let D_f be the discriminant of $f(x)$. Next, let $r_f(x) = f(x - a/3)$. Then, $r_f(x) = x^3 + Ax + B \in \mathbb{Q}[x]$ where

$$A = \frac{3b - a^2}{3}, \quad B = \frac{2a^3 - 9ab + 27c}{27} \tag{2.1}$$

and,

$$D_{r_f} = -4A^3 - 27B^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \tag{2.2}$$

From (2.1), it follows that there exist $U, V \in \mathbb{Z}$ such that $A = U/3$ and $B = V/27$ where

$$U = 3b - a^2 \ \text{ and } \ V = 2a^3 - 9ab + 27c. \tag{2.3}$$

Hence, we can write $r_f(x)$ in the form

$$r_f(x) = x^3 + \frac{U}{3}x + \frac{V}{27} \in \mathbb{Q}[x], \quad \text{with } \ U, V \in \mathbb{Z}.$$

Further, for any $w \in \mathbb{Z}$, let

$$f_w(x) = x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w) \tag{2.4}$$

where $f'(w)$ and $f''(w)$ denote the first and second derivatives of f at w. Then, $f_0(x) = f(x)$ and $f(x) \in \{f_w(x); w \in \mathbb{Z}\}$. Finally, observe that $r_{f_w}(x) = r_f(x)$ for any $w \in \mathbb{Z}$.

Lemma 2.1. *Let $f(x) = x^3 + ax^2 + bx + c$, $g(x) = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c} \in \mathbb{Z}[x]$. Then,* (i)*,* (ii) *and* (iii) *are equivalent:*

(i) *There exists a $w \in \mathbb{Z}$ satisfying $g(x) = f(x + w)$.*
(ii) *There exists a $w \in \mathbb{Z}$ satisfying $g(x) = f_w(x)$.*
(iii) *$r_f(x) = r_g(x)$.*

Proof. First we show that (i) is equivalent to (ii). Using Taylor's theorem, we obtain

$$f(x) = (x - w)^3 + \frac{f''(w)}{2!}(x - w)^2 + \frac{f'(w)}{1!}(x - w) + f(w)$$

for any $w \in \mathbb{Z}$. Therefore,

$$f(x + w) = x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w). \tag{2.5}$$

Combining (2.5) with (2.4), we get $f(x + w) = f_w(x)$. Hence, (i) and (ii) are equivalent.

Further we prove that (i) is equivalent to (iii). Assume that $g(x) = f(x + w)$ for some $w \in \mathbb{Z}$. Then, (2.5) yields

$$g(x) = x^3 + (3w + a)x^2 + (3w^2 + 2aw + b)x + w^3 + aw^2 + bw + c.$$

Hence,

$$\begin{aligned} r_g(x) &= g(x-(3w+a)/3) \\ &= g(x-w-a/3) = f(x-w-a/3+w) = f(x-a/3) = r_f(x). \end{aligned}$$

Finally, assume that $r_f(x) = r_g(x)$. Then, $f(x-a/3) = g(x-\overline{a}/3)$. Hence, we have $f(x-a/3+\overline{a}/3) = g(x-\overline{a}/3+\overline{a}/3) = g(x)$ and $g(x) = f(x+(\overline{a}-a)/3)$ follows. Put $w = (\overline{a}-a)/3$. Clearly, if $a \equiv \overline{a} \pmod 3$, then $w \in \mathbb{Z}$. Suppose that $a \not\equiv \overline{a} \pmod 3$. Using (2.3) we obtain $U = 3b-a^2 = 3\overline{b}-\overline{a}^2$, $V = 2a^3-9ab+27c = 2\overline{a}^3 - 9\overline{a}\overline{b} + 27\overline{c}$, which implies $a^2 \equiv \overline{a}^2 \pmod 3$ and $a^3 \equiv \overline{a}^3 \pmod 3$. This, together with the assumption $a \not\equiv \overline{a} \pmod 3$, yields a contradiction. The proof is complete. □

Corollary 2.2. *Let $f(x) = x^3+ax^2+bx+c$, $g(x) = x^3+\bar{a}x^2+\bar{b}x+\bar{c} \in \mathbb{Z}[x]$. If there exists a $w \in \mathbb{Z}$ satisfying $g(x) = f(x+w)$, then $a \equiv \overline{a} \pmod 3$.*

Let $D \in \mathbb{Z}$ and let $C_D \neq \emptyset$. For $f(x), g(x) \in C_D$ put

$$f(x) \sim g(x) \Longleftrightarrow \exists\, w \in \mathbb{Z} : g(x) = f(x+w) = f_w(x) \Longleftrightarrow r_f(x) = r_g(x).$$

It is evident that $\sim$ is an equivalence relation on the set C_D. Next, it is well-known that, if $D \neq 0$, then $C_D/\!\sim$ has only finitely many equivalence classes. This claim follows as a consequence of a more general result proved in 1973 by Kálmán György [9, p. 419]. See also [10, p. 475] or consult [4, p. 109]. György's result can be formulated as follows:

Proposition 2.3. (K. György, 1973) *Up to equivalence, there are only finitely many monic polynomials in $\mathbb{Z}[x]$ with a given non-zero discriminant and all these polynomials can be effectively determined.*

In Proposition 2.3, the equivalence of two polynomials $f(x)$, $g(x) \in \mathbb{Z}[x]$ means that there exists $w \in \mathbb{Z}$ such that $g(x) = f(x+w)$ and effectively determined means that there is an algorithm (a deterministic Turing machine) that, for any choice of input from the given set, computes the output in finitely many steps. Consult [4, p. 50].

In Section 3, we give an alternative proof of the fact that $C_D/\!\sim$ has only finitely many equivalence classes for any $0 \neq D \in \mathbb{Z}$ and, $C_D \neq \emptyset$. Our proof will be based on using the well-known result of L. J. Mordell [18] presented in the following Theorem 2.4.

Theorem 2.4. (L. J. Mordell, 1920) *For any given $0 \neq k \in \mathbb{Z}$, the equation*

$$Y^2 = X^3 + k$$

has at most finitely many integer solutions.

Let $D \in \mathbb{Z}$ and let $f(x) = x^3+ax^2+bx+c \in C_D$. Then, there are uniquely determined $w \in \mathbb{Z}$ and $e \in \{0,1,2\}$ such that $a = 3w+e$. Put

$$r(x) = f(x-w) = x^3+ex^2+(b-3w^2-2ew)x+2w^3+ew^2-bw+c. \quad (2.6)$$

The polynomial $r(x)$ will be called a canonical representative of the class

$$[f(x)] = \{g(x) \in C_D : g(x) \sim f(x)\} \in C_D/\!\sim .$$

Observe that $r_f(x)$ is a canonical representatives of $[f(x)]$ if and only if $e = 0$. Next, for any $0 \neq D \in \mathbb{Z}$, let

$$c(D) = \begin{cases} \#C_D/\sim & \text{if } C_D \neq \emptyset, \\ 0 & \text{if } C_D = \emptyset. \end{cases}$$

Finally, let R_D denote the full system of canonical representatives of $C_D/\sim$. Hence, $\#R_D = \#C_D/\sim$. The following problems (i) – (iv) will be studied in Section 3 in detail:

(i) For a given $0 \neq D \in \mathbb{Z}$, find the number $c(D)$.

(ii) Establish canonical representatives of all classes of $C_D/\sim$, i.e., find the set R_D.

(iii) Determine all polynomials in $C_D \neq \emptyset$.

(iv) Find solutions to problems (i) – (iii) also for the case of $D = 0$.

3. Method for determining the set C_D

We begin with two simple lemmas.

Lemma 3.1. *Let $0 \neq D \in \mathbb{Z}$. If Mordell's equation*

$$Y^2 = X^3 + k, \text{ with } k = -432D = -2^4 3^3 D$$

has no integer solution, then $C_D = \emptyset$.

Proof. Let $f(x) = x^3 + ax^2 + bx + c \in C_D$ and let $r_f(x) = x^3 + (U/3)x + V/27 \in \mathbb{Q}[x]$. Combining (2.1)–(2.3) we obtain $D = D_f = D_{r_f} = (-4U^3 - V^2)/27$ where $U, V \in \mathbb{Z}$. Hence, $4U^3 + V^2 = -27D$ which is equivalent to $(4V)^2 = (-4U)^3 - 432D$. Put $X = -4U$, $Y = 4V$. Then, $X, Y \in \mathbb{Z}$ and, $Y^2 = X^3 - 432D$. □

Lemma 3.2. *Let $X_0, Y_0, e \in \mathbb{Z}$ be such that*

$$4e^2 - X_0 \equiv 0 \pmod{12} \quad \text{and} \quad 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}. \tag{3.1}$$

Then, there exists exactly one $e \in \{0, 1, 2\}$ satisfying (3.1).

Proof. Let X_0, Y_0 satisfy (3.1) for some $e \in \{0, 1, 2\}$ and suppose that e is not unique. Then, $4e^2 - X_0 \equiv 0 \pmod{12}$ yields $e \in \{1, 2\}$ and $X_0 \equiv 4 \pmod{12}$. Next, using $4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}$, we obtain $Y_0 \equiv 3X_0 - 4 \equiv 6X_0 - 32 \pmod{108}$. Hence, $3X_0 \equiv 28 \pmod{108}$. By the well-known criterion on the solubility of linear congruences (see, for example [5, p. 62]), we get a contradiction. □

Before proceeding, the following notations will be adopted. For any $0 \neq D \in \mathbb{Z}$, let

$$M_D = \{[X_0, Y_0] : X_0, Y_0 \in \mathbb{Z} \text{ and } Y_0^2 = X_0^3 - 432D\},$$

$$E_D = \{[[X_0, Y_0], e] \in M_D \times \{0, 1, 2\} : 4e^2 - X_0 \equiv 0 \pmod{12}, 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}\}.$$

Theorem 3.3. *Let $0 \neq D \in \mathbb{Z}$ and let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Then, $f(x) \in C_D$ if and only if there exist $w \in \mathbb{Z}$ and $[[X_0, Y_0], e] \in E_D$ such that*

$$a = 3w + e, \tag{3.2}$$

$$b = 3w^2 + 2ew + \frac{4e^2 - X_0}{12}, \tag{3.3}$$

$$c = w^3 + ew^2 + \frac{4e^2 - X_0}{12}w + \frac{4e^3 - 3eX_0 + Y_0}{108}. \tag{3.4}$$

Moreover, if $f(x) \in C_D$, *then*

$$r(x) = f(x - w) = x^3 + ex^2 + \frac{4e^2 - X_0}{12}x + \frac{4e^3 - 3eX_0 + Y_0}{108} \tag{3.5}$$

is a canonical representative of the class $[f(x)]$.

Proof. Let $f(x) = x^3 + ax^2 + bx + c \in C_D$. Then, $r_f(x) = x^3 + (U/3)x + V/27 \in \mathbb{Q}[x]$ where $U, V \in \mathbb{Z}$ such that $U = 3b - a^2$ and, $V = 2a^3 - 9ab + 27c$. From Lemma 3.1 now it follows that there exists a $[X_0, Y_0] \in M_D$ satisfying

$$X_0 = -4U \text{ and, } Y_0 = 4V. \tag{3.6}$$

Since $a \in \mathbb{Z}$, there are uniquely determined $w \in \mathbb{Z}$ and $e \in \{0, 1, 2\}$ such that $a = 3w + e$. Substituting $a = 3w + e$ into $U = 3b - a^2$, we obtain $U \equiv -e^2 \pmod 3$. Since $X_0 = -4U$, by (3.6), we have $4e^2 - X_0 \equiv 0 \pmod{12}$.

Further, substituting $a = 3w + e$ and $3b = U + (3w + e)^2$ into $V = 2a^3 - 9ab + 27c$, after some calculations, we obtain

$$V = -27(w^3 + ew^2 - c) - 9w(U + e^2) - e^3 - 3eU. \tag{3.7}$$

Since $U + e^2 \equiv 0 \pmod 3$, from (3.7) it follows that

$$V \equiv -e^3 - 3eU \pmod{27}.$$

This, together with (3.6) yields $4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}$, as required.

Conversely, assume that $w \in \mathbb{Z}$ and $[[X_0, Y_0], e] \in E_D$. Next, let a, b, c be defined by (3.2), (3.3), (3.4). Then, $a, b, c \in \mathbb{Z}$ and $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. We will prove that $D_f = D$. Substituting (3.2) and, (3.3) into $U = 3b - a^2$, we get $U = -X_0/4$. Similarly, substituting (3.2), (3.3) and, (3.4) into $V = 2a^3 - 9ab + 27c$, we get $V = Y_0/4$. Hence,

$$r_f(x) = x^3 + \frac{U}{3}x + \frac{V}{27} = x^3 - \frac{X_0}{12}x + \frac{Y_0}{108}. \tag{3.8}$$

From (3.8) it follows that

$$D_{r_f} = \frac{X_0^3 - Y_0^2}{432}. \tag{3.9}$$

Since $[X_0, Y_0] \in M_D$, we have $X_0^3 - Y_0^2 = 432D$. This, together with (3.9) and $D_{r_f} = D_f$ yields $D_f = D$. Finally, from (2.6) we get (3.5). The proof is complete. □

Proposition 3.4. *Let* $0 \neq D \in \mathbb{Z}$. *Then,* (i) *and* (ii) *hold:*

(i) E_D *is a finite set.*

(ii) $C_D/\sim$ *has only finitely many equivalence classes for any* $C_D \neq \emptyset$.

Proof. Conclusion (i) is a direct consequence of Theorem 2.4. (ii) Let $\varphi : E_D \to C_D/\sim$ be the mapping defined by $\varphi([[X_0, Y_0], e]) = \{f_w(x) : w \in \mathbb{Z}\}$ where

$$f_0(x) = x^3 + ex^2 + \frac{4e^2 - X_0}{12}x + \frac{4e^3 - 3eX_0 + Y_0}{108}.$$

Then, φ is bijective. Injectivity of φ is evident and surjectivity of φ immediately follows from Theorem 3.3. Hence, $\#C_D/\sim = \#E_D$. This proves (ii). □

The following convention regarding the designation of polynomials in R_D will be useful. Any triple $[e, u, v]$ will be considered a simplified expression of polynomial $x^3 + ex^2 + ux + v$. Now we are ready to describe our method for determining the set C_D. It can be formally divided into four steps as follows:

(i) Let $0 \neq D \in \mathbb{Z}$. We find the set M_D of all integer solutions $[X_0, Y_0]$ of Mordell's equation $Y^2 = X^3 - 432D$. By Theorem 2.4, M_D is a finite set and, by Lemma 3.1, if $M_D = \emptyset$, then $C_D = \emptyset$.

(ii) Let $M_D \neq \emptyset$. We determine the set E_D: For each $[X_0, Y_0] \in M_D$ we decide whether there is $e \in \{0, 1, 2\}$ satisfying $4e^2 - X_0 \equiv 0 \pmod{12}$ and, $4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}$. By Lemma 3.2, no more than one number e meets the above conditions. Since $\#E_D = \#C_D/\sim$, we have $C_D = \emptyset$ if and only if $E_D = \emptyset$.

(iii) Let $E_D \neq \emptyset$. We construct the set R_D, i.e. the full system of representatives of $C_D/\sim$. Under the above convention, we have

$$R_D = \left\{ \left[e, \frac{4e^2 - X_0}{12}, \frac{4e^3 - 3eX_0 + Y_0}{108} \right] : [[X_0, Y_0], e] \in E_D \right\}.$$

(iv) Finally, using Lemma 2.1, we get

$$C_D = \bigcup_{g \in R_D} \left\{ x^3 + \frac{g''(w)}{2!}x^2 + \frac{g'(w)}{1!}x + g(w) : w \in \mathbb{Z} \right\}.$$

The below example illustrates our method.

Example 3.5. Let $D = 29$. In the first step, we find the set

$$M_{29} = \{[24, \pm 36], [33, \pm 153], [112, \pm 1180], [384, \pm 7524], [528, \pm 12132]\}.$$

Hence, $\#M_{29} = 10$. Next, we determine that

$$E_{29} = \{[[112, -1180], 1], [[112, 1180], 2]\}.$$

Third, we establish the set R_{29} of all canonical representatives of $C_{29}/\sim$.

$$R_{29} = \{x^3 + x^2 - 9x - 14,\ x^3 + 2x^2 - 8x + 5\}.$$

Under our convention, we can write R_{29} briefly as $R_{29} = \{[1, -9, -14], [2, -8, 5]\}$. Hence, $c(29) = \#C_{29}/\sim = 2$. Finally, we find

$$C_{29} = \bigcup_{g \in R_{29}} \left\{ x^3 + \frac{g''(w)}{2!}x^2 + \frac{g'(w)}{1!}x + g(w) : w \in \mathbb{Z} \right\}.$$

In particular, we have

$$C_{29} = \{x^3 + (3w + 1)x^2 + (3w^2 + 2w - 9)x + w^3 + w^2 - 9w - 14 : w \in \mathbb{Z}\} \cup$$
$$\{x^3 + (3w + 2)x^2 + (3w^2 + 4w - 8)x + w^3 + 2w^2 - 8w + 5 : w \in \mathbb{Z}\}.$$

Applying the method, the validity of Theorem 3.6 can be verified.

Theorem 3.6. *Let $0 \neq D \in \mathbb{Z}$ and let $1 \leq |D| \leq 1000$. Then, we have:*
(i) *If $-1 \geq D \geq -1000$, then $C_D \neq \emptyset$ if and only if*

$$\begin{aligned}D \in \{&-3,-4,-16,-23,-27,-28,-31,-32,-44,-59,-72,-76,-83,-87,\\ &-99,-100,-104,-107,-108,-112,-116,-135,-139,-140,-147,-152,\\ &-172,-175,-176,-192,-199,-200,-204,-211,-212,-216,-231,-236,\\ &-239,-240,-243,-244,-247,-255,-256,-268,-275,-279,-283,-288,\\ &-300,-304,-307,-324,-327,-331,-332,-335,-339,-351,-356,-364,\\ &-367,-379,-400,-411,-416,-419,-424,-428,-432,-436,-439,-440,\\ &-448,-451,-459,-460,-464,-472,-475,-484,-491,-492,-499,-500,\\ &-507,-515,-519,-524,-527,-540,-543,-547,-556,-560,-563,-567,\\ &-575,-588,-608,-620,-643,-652,-655,-671,-675,-679,-680,-684,\\ &-687,-688,-695,-696,-707,-716,-720,-728,-731,-743,-744,-748,\\ &-751,-755,-759,-771,-780,-783,-800,-804,-808,-812,-815,-816,\\ &-823,-828,-835,-839,-843,-844,-848,-863,-864,-867,-876,-883,\\ &-888,-891,-907,-931,-932,-940,-944,-948,-959,-968,-972,-976,\\ &-983,-984,-996\}.\end{aligned}$$

(ii) *If $1 \leq D \leq 1000$, then $C_D \neq \emptyset$ if and only if*

$$\begin{aligned}D \in \{&4,5,8,12,13,20,21,29,32,36,40,45,48,49,53,60,68,77,81,85,96,104,\\ &108,112,117,125,132,140,144,148,164,165,169,173,176,189,192,200,216,\\ &221,224,228,229,252,256,257,260,272,285,288,292,293,316,320,321,328,\\ &328,333,356,357,361,365,368,392,396,400,404,432,437,445,452,468,469,\\ &473,480,488,500,512,516,525,528,533,544,549,564,568,572,580,592,600,\\ &605,608,621,629,644,656,672,680,684,697,708,725,729,733,752,756,761,\\ &768,780,785,788,792,816,832,837,845,864,868,892,896,900,904,916,932,\\ &940,957,965,981,985,992,993\}.\end{aligned}$$

The following proposition reveals some important properties of the set R_D. First observe that, if $f(x) = x^3 + ex^2 + ux + v \in \mathbb{Z}[x]$ with $e \in \{0,1,2\}$, then

$$f(x) \in C_D \text{ if and only if } f(x) \in R_D. \tag{3.10}$$

Proposition 3.7. *Let $0 \neq D \in \mathbb{Z}$. Then,* (i) *and* (ii) *hold:*
(i) $[0,u,v] \in R_D$ *if and only if* $[0,u,-v] \in R_D$.
(ii) $[1,u,v] \in R_D$ *if and only if* $[2,u+1,u-v] \in R_D$.
Moreover, in (i), $[0,u,v]$ *is not equivalent to* $[0,u,-v]$ *for any* $v \neq 0$. *Similarly, in* (ii), $[1,u,v]$ *is not equivalent to* $[2,u+1,u-v]$.

Proof. (i) Let $f(x) = x^3 + ux + v$ and let $g(x) = x^3 + ux - v$. Then, $D_f = D_g = -4u^3 - 27v^2$. This together with (3.10) yields (i). Suppose now that $v \neq 0$ and that $g(x) = f(x+w)$ for some $w \in \mathbb{Z}$. Then,

$$x^3 + ux + v = x^3 + 3wx^2 + (3w^2 + u)x + w^3 + ux + v.$$

Matching coefficients on both sides of the equation, we obtain $v = 0$, a contradiction.

(ii) Let $f(x) = x^3 + x^2 + ux + v$ and let $g(x) = x^3 + 2x^2 + (u+1)x + u - v$. By direct calculation we obtain $D_f = D_g = -4u^3 + u^2 - 27v^2 + 18uv - 4v$. This,

together with (3.10) yields (ii). Finally, the claim that $[1,u,v]$ is not equivalent to $[2,u+1,u-v]$ follows immediately from Corollary 2.2. □

Note that part (ii) of Proposition 3.7 can be formulated in an equivalent form as follows: $[2,r,s] \in R_D$ if and only if $[1,r-1,r-s-1] \in R_D$. Next, it is clear that relations (i) and (ii) in Proposition 3.7 have practical significance. For example, if we know that $[1,-3077,64681] \in R_{-76}$, then $[2,-3076,-67758] \in R_{-76}$ as well.

We conclude Section 3 with a complete solution of the case $D=0$. The following definition will be useful. Let $M_0 = \{[X_0,Y_0] : X_0, Y_0 \in \mathbb{Z}, Y_0^2 = X_0^3\}$. First observe that

$$M_0 = \{[\alpha^2,\alpha^3] : \alpha \in \mathbb{Z}\}. \tag{3.11}$$

The inclusion $\{[\alpha^2,\alpha^3] : \alpha \in \mathbb{Z}\} \subseteq M_0$ is evident while the reverse inclusion is a simple consequence of unique prime factorization of X_0 and Y_0.

Theorem 3.8. *Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Then, $f(x) \in C_0$ if and only if there exist $e \in \{0,1,2\}$, $v,w \in \mathbb{Z}$ such that*

$$\begin{aligned} f(x) = x^3 &+ (3w+e)x^2 + (3w^2 + 2ew - 3v^2 - 2ev)x + w^3 + ew^2 \\ &- (3v^2 + 2ev)w + 2v^3 + ev^2 = (x+w-v)^2(x+w+2v+e). \end{aligned} \tag{3.12}$$

Consequently, $C_0/\!\sim$ has infinitely many classes and R_0 can be written in the form

$$R_0 = \{[e, -3v^2 - 2ev, 2v^3 + ev^2] : e \in \{0,1,2\}, v \in \mathbb{Z}\}.$$

Proof. Let $f(x) = x^3 + ax^2 + bx + c \in C_0$ and, let $r_f(x) = x^3 + (U/3)x + V/27$ where $U,V \in \mathbb{Z}$. Then, $4U^3 + V^2 = 0$, which yields $(4V)^2 = (-4U)^3$. Put $X = -4U$ and, $Y = 4V$. Then, $X,Y \in \mathbb{Z}$ and, $Y^2 = X^3$. From (3.11) now it follows that $[X,Y] = [\alpha^2,\alpha^3]$ for some $\alpha \in \mathbb{Z}$. Consequently, $\alpha^2 = -4U$ and, $\alpha^3 = 4V$. This means that, there is a $u \in \mathbb{Z}$ such that $\alpha = 2u$. Hence, $U = -u^2$, $V = 2u^3$ and, $r_f(x) = x^3 - (u^2/3)x + 2u^3/27$. Since $u \in \mathbb{Z}$, there are uniquely determined $v \in \mathbb{Z}$ and $e \in \{0,1,2\}$ satisfying $u = 3v + e$. Put $g(x) = r_f(x + e/3)$. Simple calculation yields that

$$g(x) = x^3 + ex^2 - (3v^2 + 2ev)x + 2v^3 + ev^2 = (x-v)^2(x+2v+e). \tag{3.13}$$

Combining (3.13) and (3.10), we obtain $g(x) \in R_0$. Finally, for any $w \in \mathbb{Z}$, we have $f(x) = g(x+w)$ and (3.12) follows.

Conversely, let $f(x) \in \mathbb{Z}[x]$ satisfy (3.12) for some $e \in \{0,1,2\}$ and $v,w \in \mathbb{Z}$. Since $v - w$ is a multiple root of $f(x)$, we see immediately that $D_f = 0$. Hence, $f(x) \in C_0$. □

4. Application of the method for $1 \le |D| \le 1000$

In this section we summarize some results obtained using a computer for the values of D in the range $1 \le |D| \le 1000$. Let

$$\mathbb{D}(-1000) = \{D \in \mathbb{Z} : -1 \ge D \ge -1000\}$$

and,

$$\mathbb{D}(1000) = \{D \in \mathbb{Z} : 1 \le D \le 1000\}.$$

Next, for any $n \in \mathbb{N} \cup \{0\}$, let

$$N_n := \#\{D \in \mathbb{D}(-1000) : \#M_D = n\} \quad \text{and,} \quad P_n := \#\{D \in \mathbb{D}(1000) : \#M_D = n\}.$$

For N_n and P_n, the following results have been obtained:

Table 1

n	0	1	2	4	5	6	8	9	10	12	14	16	18	20	22	26
N_n	611	4	270	56	1	19	9	1	9	6	5	4	1	3	1	0
P_n	745	5	154	41	1	30	7	0	6	2	4	3	1	0	0	1

Further, for any $n \in \mathbb{N} \cup \{0\}$, let

$$\alpha_n := \#\{D \in \mathbb{D}(-1000) : c(D) = n\} \quad \text{and,} \quad \beta_n := \#\{D \in \mathbb{D}(1000) : c(D) = n\}.$$

Then, we have:

Table 2

n	0	1	2	4	5	6	7	8	10	12	14
α_n	839	4	90	44	1	13	1	6	2	0	0
β_n	870	5	88	16	1	8	0	5	3	3	1

Observe that, according to Table 1, approximately 68% of the values $1 \leq |D| \leq 1000$ do not meet the necessary condition for $C_D \neq \emptyset$ given in Lemma 3.1. Next, according to Table 2, approximately 85.5% of all values of $1 \leq |D| \leq 1000$ yield $C_D = \emptyset$. This fact also follows from (i) and (ii) of Theorem 3.6.

Now we focus on the arithmetic properties of integer solutions of Mordell's equation (1.1) with $k = -432D$.

Lemma 4.1. *Let $0 \neq D \in \mathbb{Z}$ and let $[X_0, Y_0] \in M_D$. Then,* (i), (ii), (iii), *and* (iv) *hold:*

(i) *If $2|X_0$, then $4|X_0$, $4|Y_0$.*
(ii) *If $2|Y_0$, then $4|X_0$, $4|Y_0$.*
(iii) *If $3|X_0$, then $9|Y_0$.*
(iv) *If $3|Y_0$, then $3|X_0$, $9|Y_0$.*

Proof. The conclusions (i)–(iv) immediately follow from $Y_0^2 = X_0^3 - 432D$. □

Combining parts (i) and (ii) of Lemma 4.1, we see that $X_0 \equiv 0 \pmod 2$ if and only if $Y_0 \equiv 0 \pmod 2$. Hence, the following two definitions are possible:

(i) A solution $[X_0, Y_0] \in M_D$ is called even, if X_0 and Y_0 are even.
(ii) A solution $[X_0, Y_0] \in M_D$ is called odd, if X_0 and Y_0 are odd.

Next, for any $0 \neq D \in \mathbb{Z}$, let

$$\mathcal{E}_D = \{[X_0, Y_0] \in M_D : X_0 \equiv Y_0 \equiv 0 \pmod 2\},$$
$$\mathcal{O}_D = \{[X_0, Y_0] \in M_D : X_0 \equiv Y_0 \equiv 1 \pmod 2\}.$$

Then, $\mathcal{E}_D \cap \mathcal{O}_D = \emptyset$ and, $\mathcal{E}_D \cup \mathcal{O}_D = M_D$. Finally, for any positive integer n, put

$$\varepsilon_n = \sum_{D=1}^{n} \#\mathcal{E}_D, \quad \varepsilon_{-n} = \sum_{D=-1}^{-n} \#\mathcal{E}_D, \quad o_n = \sum_{D=1}^{n} \#\mathcal{O}_D, \quad o_{-n} = \sum_{D=-1}^{-n} \#\mathcal{O}_D \quad \text{and,}$$

$$\sigma_n = \sum_{D=1}^{n} \#M_D = \varepsilon_n + o_n, \quad \sigma_{-n} = \sum_{D=-1}^{-n} \#M_D = \varepsilon_{-n} + o_{-n}.$$

Computer investigation of the values ε_n, ε_{-n}, o_n and o_{-n} for $n \leq 1000$ reveals a significant difference between the numbers of even and odd solutions in the investigated range. We have found

$$\varepsilon_{-1000} = 916, \quad \varepsilon_{1000} = 638, \quad o_{-1000} = 448 \text{ and, } \quad o_{1000} = 312. \tag{4.1}$$

From (4.1) it follows that there exist approximately 67% even and only 33% odd integer solutions of $Y^2 = X^3 - 432D$ for $0 \neq |D| \leq 1000$. This leads to a natural question that can be formulated as Problem 4.2.

Problem 4.2. Prove or disprove (4.2).

$$\lim_{n\to\infty} \frac{\varepsilon_n}{\sigma_n} = \lim_{n\to\infty} \frac{\varepsilon_{-n}}{\sigma_{-n}} = \frac{2}{3} \text{ and, } \quad \lim_{n\to\infty} \frac{o_n}{\sigma_n} = \lim_{n\to\infty} \frac{o_{-n}}{\sigma_{-n}} = \frac{1}{3}. \tag{4.2}$$

Clearly, if (4.2) holds, then we also have

$$\lim_{n\to\infty} \frac{o_n}{\varepsilon_n} = \lim_{n\to\infty} \frac{o_{-n}}{\varepsilon_{-n}} = \frac{1}{2}.$$

The ratio between the numbers of even and odd solutions is also interesting in relation to the construction of the set C_D. It follows from Theorem 3.3 that only even solutions are relevant for determining C_D.

Finally, after a short inspection of Theorem 3.6, we find that, for $1 \leq |D| \leq 1000$, the following implication holds: If $C_D \neq \emptyset$ and $C_{-D} \neq \emptyset$, then D is even. In Proposition 4.3 we prove that the validity of this implication can not only be extended to any $0 \neq D \in \mathbb{Z}$, but also strengthened.

Proposition 4.3. *Let $0 \neq D \in \mathbb{Z}$. Then,* (i) *and* (ii) *hold:*

(i) *If $C_D \neq \emptyset$ and $2|D$, then $4|D$.*
(ii) *If $C_D \neq \emptyset$ and $C_{-D} \neq \emptyset$, then $4|D$.*

Proof. (i) Let $C_D \neq \emptyset$ and let $2|D$. Then, by Theorem 3.3, there exist $X_0, Y_0 \in \mathbb{Z}$ satisfying $2|X_0$, $2|Y_0$ and $Y_0^2 = X_0^3 - 432D$. Further, by Lemma 4.1, $4|X_0$, $4|Y_0$. This means that there exist $\xi, \eta, \delta \in \mathbb{Z}$ such that $X_0 = 4\xi$, $Y_0 = 4\eta$, $D = 2\delta$. Hence, $2^4\eta^2 = 2^6\xi^3 - 2^5 3^3\delta$, which yields $2|\delta$. This proves $4|D$.

(ii) Let $C_D \neq \emptyset$ and let $C_{-D} \neq \emptyset$. Then, there exist $X_1, Y_1, X_2, Y_2 \in \mathbb{Z}$ satisfying $2|X_1$, $2|Y_1$, $2|X_2$, $2|Y_2$ and, $Y_1^2 = X_1^3 - 432D$, $Y_2^2 = X_2^3 + 432D$. Subtracting $Y_2^2 = X_2^2 + 432D$ from $Y_1^2 = X_1^2 - 432D$, we obtain

$$Y_1^2 - Y_2^2 = X_1^3 - X_2^3 - 2^5 3^3 D. \tag{4.3}$$

Next, by Lemma 4.1, we have $4|X_1$, $4|Y_1$, $4|X_2$, $4|Y_2$. Hence, $X_1^3 - X_2^3 \equiv 0 \pmod{2^6}$ and, $Y_1^2 - Y_2^2 \equiv 0 \pmod{2^4}$. Now we see that reducing (4.3) by modulus 2^5 we obtain

$$Y_1^2 - Y_2^2 \equiv (Y_1 + Y_2)(Y_1 - Y_2) \equiv 0 \pmod{2^5}.$$

Hence and from $Y_1 + Y_2 \equiv Y_1 - Y_2 \equiv 0 \pmod{2^2}$, it follows that

$$Y_1^2 - Y_2^2 \equiv 0 \pmod{2^6}. \tag{4.4}$$

Combining (4.4) with (4.3) we obtain $2^5 3^3 D \equiv 0 \pmod{2^6}$. Hence, $2|D$. This together with part (i) of Proposition 4.3 yields $4|D$, as required. □

5. Conclusion

The method presented in this paper makes it possible to determine the set C_D using the full system of canonical representatives. Creating tables of these representatives and analyzing them can lead to the discovery of new interesting facts. These tables can also be useful for a better understanding of the law of inertia for the factorization of cubic polynomials, which has been studied in [11–16].

Acknowledgement. The author thanks the anonymous referee for careful reading of the manuscript.

References

[1] M. A. Bennett and A. Ghadermarzi, *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18** (2015), 633–646.
[2] B. N. Delone and D. K. Faddeev, *Theory of irrationalities of the third degree* (in Russian), Travaux Inst. Math. Stekloff **11** (1940), 3–340.
[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. II: Diophantine analysis, Dover Publications, Mineola, New York, 2005.
[4] J. H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2017.
[5] G. H. Hardy and E. M. Wright, *An introduction to the Theory of Numbers*, 6$^{\text{th}}$ Ed., Oxford University Press, New York, 2008.
[6] O. Hemer, *On the Diophantine Equation* $y^2 - k = x^3$, Doctoral Dissertation, Uppsala, 1952.
[7] S. Gauthier and F. Lê, *On the youthful writings of Louis J. Mordell on the Diophantine equation* $y^2 - k = x^3$, Arch. Hist. Exact Sci. **73** (2019), 427–468.
[8] J. Gebel, A. Pethö and G. H. Zimmer, *On Mordell's equation*, Compos. Math. **110** (1998), 335–367.
[9] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426.
[10] K. Győry, *Polynomials and binary forms with given discriminant*, Publ. Math. **69** (2006), 473–499.
[11] J. Klaška and L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49** (2011), 310–319.
[12] J. Klaška and L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Util. Math. **102** (2017), 39–50.
[13] J. Klaška and L. Skula, *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Util. Math. **103** (2017), 99–109.
[14] J. Klaška and L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66** (2016), 1019–1027.
[15] J. Klaška and L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of primes* 2 *and* 3, Math. Slovaca **67** (2017), 71–82.
[16] J. Klaška and L. Skula, *On the factorizations of cubic polynomials with the same discriminant modulo a prime*, Math. Slovaca **68** (2018), 987–1000.
[17] J. London and M. Finkelstein, *On Mordell's Equation* $y^2 - k = x^3$, Bowling Green, Ohio Bowling Green State University, 1973.
[18] L. J. Mordell, *A statement by Fermat*, Proc. Lond. Math. Soc. (2) **18** (1920), v–vi.
[19] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1998.

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