DE GRUYTER

Mathematica Slovaca

DOI: 10.1515/ms-2022-0003
Math. Slovaca **72** (2022), No. 1, 35–50

QUARTIC POLYNOMIALS WITH A GIVEN DISCRIMINANT

Jiří Klaška

Dedicated to the eminent Czechoslovak mathematician Ladislav Skula

(*Communicated by Milan Paštéka*)

ABSTRACT. Let $0 \neq D \in \mathbb{Z}$ and let Q_D be the set of all monic quartic polynomials $x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ with the discriminant equal to D. In this paper we will devise a method for determining the set Q_D. Our method is strongly related to the theory of integral points on elliptic curves. The well-known Mordell's equation plays an important role as well in our considerations. Finally, some new conjectures will be included inspired by extensive calculations on a computer.

1. Introduction

Let $0 \neq D \in \mathbb{Z}$ and let

$$Q_D = \{f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]; D_f = D\} \tag{1.1}$$

where

$$\begin{aligned} D_f &= a^2b^2c^2 - 4a^2b^3d - 4a^3c^3 + 18a^3bcd - 27a^4d^2 - 4b^3c^2 \\ &\quad + 16b^4d + 18abc^3 - 80ab^2cd - 6a^2c^2d + 144a^2bd^2 \\ &\quad - 27c^4 + 144bc^2d - 128b^2d^2 - 192acd^2 + 256d^3 \end{aligned} \tag{1.2}$$

is the discriminant of $f(x)$. In this paper, the set Q_D will be studied in detail. Most of the focus will be given to the problem of determining all polynomials in Q_D. Clearly, this is equivalent to finding all integer solutions of the Diophantine equation $D_f = D$. In proving the main results, the following two known theorems will be needed.

Theorem 1.1 (Mordell, 1920). *For any given $0 \neq k \in \mathbb{Z}$, the equation*

$$Y^2 = X^3 + k \tag{1.3}$$

has at most finitely many integer solutions.

Equation (1.3) is often called Mordell's equation, in honour of the contribution Louis Joel Mordell [17] has made to this subject. An extension to Theorem 1.1 was later made by Carl Ludwig Siegel [18]. In its simplest form, Siegel's result can be formulated as follows:

Theorem 1.2 (Siegel, 1929). *Let $\alpha, \beta \in \mathbb{Z}$ be such that $4\alpha^3 + 27\beta^2 \neq 0$. Then the equation*

$$\eta^2 = \xi^3 + \alpha\xi + \beta \tag{1.4}$$

has at most finitely many integer solutions.

2020 Mathematics Subject Classification: Primary 11D25, 11D45, 11Y50.
Keywords: Quartic polynomial, discriminant, Mordell's equation, elliptic curve.

There is a standard method for computing all integer solutions of (1.3) and (1.4) 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).

Remark 1.3. Mordell's equation has had a long history. First discoveries concerning (1.3) were given in Dickson [2: pp. 533–539] going back to the work of Bachet from 1621. Many interesting historical notes to (1.3) can be found in [1,5,7,16]. Perhaps the most extensive historical comments related to Mordell's contribution to (1.3) can be found in the recent paper [6].

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 Q_D

Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ and let D_f be the discriminant of $f(x)$. Next, let $r_f(x) = f(x - a/4)$. Then

$$r_f(x) = x^4 + Ax^2 + Bx + C \in \mathbb{Q}[x] \tag{2.1}$$

where

$$A = b - \frac{3a^2}{8}, \quad B = c - \frac{ab}{2} + \frac{a^3}{8}, \quad C = d - \frac{ac}{4} + \frac{a^2b}{16} - \frac{3a^4}{256}. \tag{2.2}$$

Moreover, we have

$$D_{r_f} = D_f = 16A^4C - 4A^3B^2 - 27B^4 - 128A^2C^2 + 144AB^2C + 256C^3. \tag{2.3}$$

From (2.2), it follows that there exist $R, S, T \in \mathbb{Z}$ such that

$$A = \frac{R}{8}, \quad B = \frac{S}{8}, \quad C = \frac{T}{256}, \tag{2.4}$$

where

$$R = 8b - 3a^2, \quad S = 8c - 4ab + a^3, \quad T = 256d - 64ac + 16a^2b - 3a^4. \tag{2.5}$$

Hence, we can write (2.1) in the form

$$r_f(x) = x^4 + \frac{R}{8}x^2 + \frac{S}{8}x + \frac{T}{256} \in \mathbb{Q}[x] \quad \text{with} \quad R, S, T \in \mathbb{Z}. \tag{2.6}$$

We start with a more general theorem.

Theorem 2.1. *Let $n \in \mathbb{N}$, $n \geq 2$, $0 \neq D \in \mathbb{Z}$ and let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

be an arbitrary polynomial with the discriminant equal to D. Further, for any $w \in \mathbb{Z}$, let

$$f_w(x) = \sum_{k=0}^{n} \frac{f^{(k)}(w)}{k!} x^k, \tag{2.7}$$

where $f^{(k)}(w)$ denotes the k-th derivative of $f(x)$ at w. Then $f_w(x) \in \mathbb{Z}[x]$ and all polynomials in $\{f_w(x); w \in \mathbb{Z}\}$ have the same discriminant equal to D.

Proof. First, by induction on k, it can be proved that $k!|f^{(k)}(w)$ for any $k \in \{0,1,2,\dots\}$. Hence, $f_w(x) \in \mathbb{Z}[x]$. Further, Taylor's theorem yields

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(w)}{k!}(x-w)^k \quad \text{for any } w \in \mathbb{Z}. \tag{2.8}$$

Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ in the set of complex numbers $\mathbb{C}$. Then

$$D = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\alpha_j - \alpha_i)^2.$$

Next, by (2.8), for any $\alpha \in \{\alpha_1, \dots, \alpha_n\}$, we have

$$f(\alpha) = \sum_{k=0}^{n} \frac{f^{(k)}(w)}{k!}(\alpha - w)^k = 0. \tag{2.9}$$

Combining (2.7) with (2.9), we get $f_w(\alpha - w) = 0$, and thus,

$$\beta_1 = \alpha_1 - w, \ \dots, \ \beta_n = \alpha_n - w \tag{2.10}$$

are the roots of $f_w(x)$ in $\mathbb{C}$. Using (2.10), we now get

$$D_{f_w} = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\beta_j - \beta_i)^2 = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\alpha_j - w - (\alpha_i - w))^2 = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\alpha_j - \alpha_i)^2 = D,$$

as desired. □

Remark 2.2. Observe that, in Theorem 2.1, $f(x) = f_0(x)$. Hence, $f(x) \in \{f_w(x); w \in \mathbb{Z}\}$.

Corollary 2.3. *Let $0 \neq D \in \mathbb{Z}$ and let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q_D$. Further, for any $w \in \mathbb{Z}$, let*

$$f_w(x) = x^4 + \frac{f'''(w)}{3!}x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w). \tag{2.11}$$

Then (i) *and* (ii) *hold:*

(i) *Q_D is an infinite set and $\{f_w(x); w \in \mathbb{Z}\} \subseteq Q_D$.*

(ii) *For any $w \in \mathbb{Z}$, we have $r_{f_w}(x) = r_f(x) = x^4 + Ax^2 + Bx + C \in \mathbb{Q}[x]$, where A, B, C satisfy* (2.2).

Proof. Part (i) of Corollary 2.3 is a direct consequence of Theorem 2.1 for $n = 4$. Part (ii) can be verified by direct calculation. □

Lemma 2.4. *Let $0 \neq D \in \mathbb{Z}$ and let $f(x), g(x) \in Q_D$. Then* (i), (ii) *and* (iii) *are equivalent:*

(i) *There exists $w \in \mathbb{Z}$ satisfying $g(x) = f(x + w)$.*

(ii) *There exists $w \in \mathbb{Z}$ satisfying $g(x) = f_w(x)$.*

(iii) *$r_f(x) = r_g(x)$.*

Proof. Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$, $g(x) = x^4 + \overline{a}x^3 + \overline{b}x^2 + \overline{c}x + \overline{d} \in Q_D$.

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

$$f(x) = (x-w)^4 + \frac{f'''(w)}{3!}(x-w)^3 + \frac{f''(w)}{2!}(x-w)^2 + \frac{f'(w)}{1!}(x-w) + f(w)$$

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

$$f(x+w) = x^4 + \frac{f'''(w)}{3!}x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w). \tag{2.12}$$

Combining (2.12) with (2.11), 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 (2.12) yields

$$g(x) = x^4 + (4w+a)x^3 + (6w^2+3aw+b)x^2 + (4w^3+3aw^2+2bw+c)x + w^4 + aw^3 + bw^2 + cw + d.$$

Hence, $r_g(x) = g(x-(4w+a)/4) = g(x-w-a/4) = f(x-w-a/4+w) = f(x-a/4) = r_f(x)$.

Finally, let $r_f(x) = r_g(x)$. Then $f(x-a/4) = g(x-\overline{a}/4)$. Hence, $f(x-a/4+\overline{a}/4) = g(x-\overline{a}/4+\overline{a}/4) = g(x)$ and $g(x) = f(x-(\overline{a}-a)/4)$ follows. Put $w = (\overline{a}-a)/4$. Clearly, if $a \equiv \overline{a} \pmod 4$, then $w \in \mathbb{Z}$. Suppose that $a \not\equiv \overline{a} \pmod 4$. Using (2.5) we obtain $R = 8b-3a^2 = 8\overline{b}-3\overline{a}^2$, $S = 8c-4ab+a^3 = 8\overline{c}-4\overline{a}\overline{b}+\overline{a}^3$, which implies $a^2 \equiv \overline{a}^2 \pmod 8$ and $a^3 \equiv \overline{a}^3 \pmod 4$. Therefore, $a^2 \equiv \overline{a}^2 \pmod 4$, which yields, without loss of generality, that either $a \equiv 0 \pmod 4$, $\overline{a} \equiv 2 \pmod 4$ or $a \equiv 1 \pmod 4$, $\overline{a} \equiv 3 \pmod 4$. If $a \equiv 0 \pmod 4$, $\overline{a} \equiv 2 \pmod 4$, then $a^2 \equiv 0 \pmod 8$, $\overline{a}^2 \equiv 4 \pmod 8$, which is in contradiction to $a^2 \equiv \overline{a}^2 \pmod 8$. Similarly, if $a \equiv 1 \pmod 4$, $\overline{a} \equiv 3 \pmod 4$, then $a^3 \equiv 1 \pmod 4$, $\overline{a}^3 \equiv 3 \pmod 4$, which is in contradiction to $a^3 \equiv \overline{a}^3 \pmod 4$. □

Let $0 \neq D \in \mathbb{Z}$ and let $Q_D \neq \emptyset$. For $f(x), g(x) \in Q_D$ put

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

It is evident that $\sim$ is an equivalence relation on the set Q_D. Moreover, $Q_D/{\sim}$ has only finitely many equivalence classes. In Section 4, this fact will be proved using the results of Mordell and Siegel presented in Theorem 1.1 and Theorem 1.2. On the other hand, this claim also follows as a consequence of a more general theorem that has been proved by Kálmán Györy [8: p. 419]. See also [9: p. 475] or consult [3: p. 109].

3. Connection between Mordell's equation $Y^2 = X^3 - 2^{16}3^3D$ and the set Q_D

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

$$Y^2 = X^3 + k \quad \text{with} \quad k = -1769472D = -2^{16}3^3D \tag{3.1}$$

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

Proof. Let $f(x) = x^4+ax^3+bx^2+cx+d \in Q_D$ and let $r_f(x) = x^4+Ax^2+Bx+C \in \mathbb{Q}[x]$. Direct calculation will verify that (2.3) can be written in the form

$$D_{r_f} = \frac{4}{27}(A^2+12C)^3 - \frac{1}{27}(2A^3-72AC+27B^2)^2. \tag{3.2}$$

Substituting (2.4) into (3.2), after short calculation, we obtain

$$D_{r_f} = \frac{1}{1769472}\left((R^2+3T)^3 - (R^3-9RT+108S^2)^2\right). \tag{3.3}$$

Put

$$X = R^2+3T \quad \text{and} \quad Y = R^3-9RT+108S^2. \tag{3.4}$$

Then $X, Y \in \mathbb{Z}$ and (3.3) yields

$$Y^2 = X^3 + k \quad \text{where} \quad k = -1769472D_{r_f} = -2^{16}3^3D_{r_f}.$$

Since $D_{r_f} = D_f = D$, the proof is complete. □

Remark 3.2. If $x^4+ax^3+bx^2+cx+d \in Q_D$, then (2.2) yields $A, B, C \in \mathbb{Z} \iff 4|a$. In this case, we can write (3.2) in the form $V^2 = 4U^3 - 27D_{r_f}$, where $U = A^2+12C$ and $V = 2A^3-72AC+27B^2$. Hence, we have

$$(4V)^2 = (4U)^3 - 432D_{r_f}. \tag{3.5}$$

Since $D_{r_f} = D$, the substitutions $X = 4U$, $Y = 4V$ reduce (3.5) to

$$Y^2 = X^3 - 432D. \tag{3.6}$$

It is interesting that Mordell's equation (3.6) plays a fundamental role also in the theory of cubic polynomials with the same discriminant D. Consult [10: p. 313].

The following notation will be useful. For an arbitrary $0 \neq D \in \mathbb{Z}$, let M_D denote the set of all $[X_0, Y_0]$, where $X_0, Y_0 \in \mathbb{Z}$ and $Y_0^2 = X_0^3 - 2^{16}3^3D$.

Lemma 3.3. *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 $4|X_0$, $8|Y_0$.*

(ii) *If $2|Y_0$, then $4|X_0$, $8|Y_0$.*

(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 $Y_0^2 = X_0^3 - 2^{16}3^3D$. □

They will be used in Section 4 and Section 5.

4. Method for determining the set Q_D

The next lemma will be needed in the proof of Theorem 4.2.

Lemma 4.1. *Let $\xi_0, \eta_0, e \in \mathbb{Z}$ be such that*

$$\xi_0 \equiv 36e^2 \pmod{96} \quad \textit{and} \quad \eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{1728}. \tag{4.1}$$

Then we have:

(i) *$\xi_0 \equiv 0 \pmod{12}$ and $\eta_0 \equiv 0 \pmod{216}$.*

(ii) *There exists exactly one $e \in \{0, 1, 2, 3\}$ satisfying* (4.1).

Proof. (i) Since the validity of the congruence $\xi_0 \equiv 0 \pmod{12}$ is evident, we only prove that $\eta_0 \equiv 0 \pmod{216}$. First, observe that $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{216}$. Further, $\xi_0 \equiv 36e^2 \pmod{96}$ is equivalent to $9\xi_0 \equiv 324e^2 \pmod{864}$. Hence, $9\xi_0 \equiv 108e^2 \pmod{216}$. This, together with $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{216}$, yields $\eta_0 \equiv 0 \pmod{216}$.

(ii) Let $\xi_0, \eta_0 \in \mathbb{Z}$ satisfy (4.1) for some $e \in \{0, 1, 2, 3\}$. Suppose that e is not unique. Then it follows from $\xi_0 \equiv 36e^2 \pmod{96}$ that $e \in \{1, 3\}$ and that $\xi_0 \equiv 36 \pmod{96}$. On the other hand, using $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{1728}$, we obtain $9\xi_0 - 108 \equiv 27\xi_0 - 2916 \pmod{1728}$, which yields $\xi_0 \equiv 60 \pmod{96}$, a contradiction. □

The following Theorem 4.2 provides the necessary and sufficient condition for $Q_D \neq \emptyset$. In addition, Theorem 4.2 makes it possible to determine a particular polynomial in Q_D.

Theorem 4.2. *Let $0 \neq D \in \mathbb{Z}$ and let $M_D \neq \emptyset$. Then $Q_D \neq \emptyset$ if and only if there exists an $[X_0, Y_0] \in M_D$ such that the elliptic equation*

$$\eta^2 = \xi^3 - 108X_0\xi + 432Y_0 \tag{4.2}$$

has at least one integer solution $[\xi_0, \eta_0]$ satisfying conditions (4.3)–(4.5)

$$36e^2 - \xi_0 \equiv 0 \pmod{96}, \tag{4.3}$$

$$108e^3 - 9e\xi_0 + \eta_0 \equiv 0 \pmod{1728}, \tag{4.4}$$

$$432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0 \equiv 0 \pmod{110592}. \tag{4.5}$$

for some $e \in \{0, 1, 2, 3\}$. In this case,

$$g(x) = x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592} \in Q_D$$

and

$$r_g(x) = x^4 - \frac{\xi_0}{96}x^2 + \frac{\eta_0}{1728}x + \frac{144X_0 - \xi_0^2}{110592}.$$

Proof. First, assume that $Q_D \neq \emptyset$. Then there exists an $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q_D$ such that $r_f(x) = x^4 + (R/8)x^2 + (S/8)x + T/256 \in \mathbb{Q}[x]$ where R, S, T are integers satisfying (2.5). Further, from Theorem 3.1 it follows that there exists a $[X_0, Y_0] \in M_D$ such that $R^2 + 3T = X_0$ and $R^3 - 9RT + 108S^2 = Y_0$. Substituting $3T = X_0 - R^2$ into $R^3 - 9RT + 108S^2 = Y_0$, we obtain

$$4R^3 - 3X_0R + 108S^2 = Y_0, \tag{4.6}$$

and multiplying (4.6) by 432, we get

$$(216S)^2 = (-12R)^3 - 108X_0(-12R) + 432Y_0. \tag{4.7}$$

Put $\xi_0 = -12R$ and $\eta_0 = 216S$. Now, (4.7) implies immediately that $[\xi_0, \eta_0]$ is an integer solution of (4.2).

Finally, we have to prove that $[\xi_0, \eta_0]$ satisfies (4.3)–(4.5) for some $e \in \{0, 1, 2, 3\}$. Since $a \in \mathbb{Z}$, there exist uniquely determined $w \in \mathbb{Z}$ and $e \in \{0, 1, 2, 3\}$ such that $a = 4w + e$. Substituting $a = 4w + e$ into the first equation of (2.5), we obtain $R \equiv -3e^2 \pmod{8}$ and $-12R \equiv 36e^2 \pmod{96}$ follows. This together with $\xi_0 = -12R$ yields $\xi_0 \equiv 36e^2 \pmod{96}$. Hence, (4.3).

Further, from the second equation of (2.5), it follows

$$216S = 1728c - 864ab + 216a^3. \tag{4.8}$$

Putting $a = 4w + e$, $8b = R + 3a^2$, $\xi_0 = -12R$ and $\eta_0 = 216S$ into (4.8), we obtain

$$\eta_0 = 1728(c - 4w^3 - 3ew^2) + 36w(\xi_0 - 36e^2) + 9e\xi_0 - 108e^3. \tag{4.9}$$

Reducing (4.9) by modulus 1728 and using $\xi_0 \equiv 36e^2 \pmod{96}$, we get (4.4).

Finally, the third equation of (2.5) implies

$$432T = 110592d - 27648ac + 6912a^2b - 1296a^4. \tag{4.10}$$

For the left-hand side of (4.10), we have $432T = 144(X_0 - R^2) = 144X_0 - \xi_0^2$ and the right-hand side of (4.10) can be rewritten, substituting $a = 4w+e$, $8b = R+3a^2$, $8c = S+4ab-a^3$, $\xi_0 = -12R$ and $\eta_0 = 216S$ into

$$110592(d - w^4 - ew^3) - 64w(\eta_0 - 9e\xi_0 + 108e^3) - 1152w^2(36e^2 - \xi_0) - 16e\eta_0 + 72e^2\xi_0 - 432e^4.$$

Since $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{1728}$ and $\xi_0 \equiv 36e^2 \pmod{96}$, we get

$$144X_0 - \xi_0^2 \equiv -16e\eta_0 + 72e^2\xi_0 - 432e^4 \pmod{110592}.$$

Hence, (4.5).

Conversely, assume that there exists a $[X_0, Y_0] \in M_D$ such that equation (4.2) has an integer solution $[\xi_0, \eta_0]$ satisfying (4.3)–(4.5) for some $e \in \{0, 1, 2, 3\}$. Put

$$R = \frac{-\xi_0}{12}, \quad S = \frac{\eta_0}{216}, \quad T = \frac{144X_0 - \xi_0^2}{432}. \tag{4.11}$$

Then, by part (i) of Lemma 4.1, we have $R, S \in \mathbb{Z}$. We now prove that $T \in \mathbb{Z}$. From the first and third equation in (4.11) we obtain $T = (X_0 - R^2)/3$. First we show that

$$X_0 \equiv 0 \pmod 3 \iff R \equiv 0 \pmod 3. \tag{4.12}$$

Let $3|X_0$. Then, by part (iii) of Lemma 3.3, we have $9|Y_0$. Further, by (4.11), we have $3|\xi_0$ and $3^3|\eta_0$. Since $\eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0$, we also have $0 \equiv \eta_0^2 \equiv \xi_0^3 \pmod{3^5}$ and $\xi_0 \equiv 0 \pmod{3^2}$ follows. This together with $\xi_0 = -12R$ yields $3|R$.

Let $3|R$. Since $\xi_0 = -12R$, we have $3^2|\xi_0$ and $3^6|\xi_0^3$ follows. Next, by (4.11), $3^6|\eta_0^3$. Since $\eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0$, we have $432Y_0 \equiv 0 \pmod{3^5}$, and $Y_0 \equiv 0 \pmod{3^2}$ follows. By part (iv) of Lemma 3.3, we get $3|X_0$. This proves (4.12).

Further, suppose that $X_0 \equiv 2 \pmod 3$. Then from $[X_0, Y_0] \in M_D$ it follows that $Y_0^2 \equiv 2 \pmod 3$, which is a contradiction. Combining this fact with (4.12), we get

$$X_0 \equiv 1 \pmod 3 \iff R \equiv 1 \pmod 3 \quad \text{or} \quad R \equiv 2 \pmod 3 \iff R^2 \equiv 1 \pmod 3. \tag{4.13}$$

Clearly, in both cases (4.12) and (4.13), we have $X_0 - R^2 \equiv 0 \pmod 3$. Hence, $T \in \mathbb{Z}$.

Consider now the polynomial

$$r(x) = x^4 + \frac{R}{8}x^2 + \frac{S}{8}x + \frac{T}{256} \in \mathbb{Q}[x].$$

We prove that the discriminant D_r of $r(x)$ is equal to D. First, direct calculation verifies that

$$D_r = \frac{(R^2 + 3T)^3 - (R^3 - 9RT + 108S^2)^2}{2^{16}3^3}.$$

On the other hand, substituting $\xi_0 = -12R$, $\eta_0 = 216S$ into $\eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0$, we obtain

$$(216S)^2 = (-12R)^3 - 108X_0(-12R) + 432Y_0.$$

Hence, we get $R^3 - 3R(X_0 - R^2) + 108S^2 = Y_0$. Since, $X_0 - R^2 = 3T$, we have $R^3 - 9RT + 108S^2 = Y_0$. This, together with $Y_0^2 = X_0^3 - 2^{16}3^3D$ yields

$$D = \frac{(R^2 + 3T)^3 - (R^3 - 9RT + 108S^2)^2}{2^{16}3^3}.$$

Hence, $D_r = D$.

Finally, let $e \in \{0, 1, 2, 3\}$ satisfy (4.3)–(4.5). Then, by part (ii) of Lemma 4.1, e is uniquely determined. Put $g(x) = r(x + e/4)$. Then we obtain after some calculation that

$$\begin{aligned} g(x) &= x^4 + ex^3 + \frac{R + 3e^2}{8}x^2 + \frac{eR + 2S + e^3}{16}x + \frac{2e^2R + 8eS + T + e^4}{256} \\ &= x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592} \end{aligned}$$

and

$$r_g(x) = r(x) = x^4 - \frac{\xi_0}{96}x^2 + \frac{\eta_0}{1728}x + \frac{144X_0 - \xi_0^2}{110592}.$$

Since $D_g = D_{r_g} = D_r = D$, we have $g(x) \in Q_D$, as desired. The proof is complete. □

Before proceeding, the following notations will be adopted. For any $[X_0, Y_0] \in M_D$, let $E_D(X_0, Y_0)$ denote the set of all $[\xi_0, \eta_0]$ where $\xi_0, \eta_0 \in \mathbb{Z}$ and $\eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0$. Next, let E_D denote the set of all $[X_0, Y_0, \xi_0, \eta_0, e]$ where $[X_0, Y_0] \in M_D$, $[\xi_0, \eta_0] \in E_D(X_0, Y_0)$ and $e \in \{0, 1, 2, 3\}$ satisfy (4.3)–(4.5).

Corollary 4.3. *Let $0 \neq D \in \mathbb{Z}$ and let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$. Then $f(x) \in Q_D$ if and only if there exists $[X_0, Y_0, \xi_0, \eta_0, e] \in E_D$ and $w \in \mathbb{Z}$ such that*

$$\begin{aligned} a &= 4w + e,\\ b &= 6w^2 + 3ew + \frac{36e^2 - \xi_0}{96},\\ c &= 4w^3 + 3ew^2 + \frac{36e^2 - \xi_0}{48}w + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728},\\ d &= w^4 + ew^3 + \frac{36e^2 - \xi_0}{96}w^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}w + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}. \end{aligned}$$

Proposition 4.4. *Let $0 \neq D \in \mathbb{Z}$ and let $M_D \neq \emptyset$. Then* (i), (ii) *and* (iii) *hold:*

(i) *$E_D(X_0, Y_0)$ is a finite set for any $[X_0, Y_0] \in M_D$.*

(ii) *E_D is a finite set.*

(iii) *$Q_D/\!\sim$ has only finitely many equivalence classes for any $Q_D \neq \emptyset$.*

Proof. (i) Put $\alpha = -108X_0$ and $\beta = 432Y_0$. Then $4\alpha^3 + 27\beta^2 = 2^8 3^9(-X_0^3 + Y_0^2) = -2^{24}3^{12}D \neq 0$. Conclusion (i) now follows from Theorem 1.2.

(ii) Conclusion (ii) is a direct consequence of Theorem 1.1 and part (i) of Proposition 4.4.

(iii) Let $\varphi : E_D \to Q_D/\!\sim$ be the mapping defined by $\varphi(X_0, Y_0, \xi_0, \eta_0, e) = \{f_w(x); w \in \mathbb{Z}\}$, where

$$f_0(x) = x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}.$$

Then φ is bijective. Injectivity of φ is evident and surjectivity of φ immediately follows from Corollary 4.3. Hence, $\#Q_D/\!\sim = \#E_D$. This proves (iii). □

Remark 4.5. Let $[X_0, Y_0], [X_0^*, Y_0^*] \in M_D$ and let $[X_0, Y_0] \neq [X_0^*, Y_0^*]$. By an example we will prove that the set $E_D(X_0, Y_0) \cap E_D(X_0^*, Y_0^*)$ can be nonempty. For $D = -23$, we have $[64, 6400], [-320, -2816] \in M_{-23}$ and $[96, \pm 1728] \in E_{-23}(64, 6400) \cap E_{-23}(-320, -2816)$.

Now we are ready to formulate the method for determining the set Q_D. It can be formally divided into five steps as follows:

(i) Let $0 \neq D \in \mathbb{Z}$. First we find the set M_D of all integer solutions $[X_0, Y_0]$ of Mordell's equation $Y^2 = X^3 - 2^{16}3^3D$. By Theorem 1.1, M_D is a finite set and Theorem 3.1 states that, if $M_D = \emptyset$, then $Q_D = \emptyset$.

(ii) Let $M_D \neq \emptyset$. Next we find, for any $[X_0, Y_0] \in M_D$, the set $E_D(X_0, Y_0)$ of all integer solutions $[\xi_0, \eta_0]$ of the elliptic equation $\eta^2 = \xi^3 - 108X_0\xi + 432Y_0$. By part (i) of Proposition 4.4, $E_D(X_0, Y_0)$ is a finite set for any $[X_0, Y_0] \in M_D$ and Theorem 4.2 says that, if $E_D(X_0, Y_0) = \emptyset$ for any $[X_0, Y_0] \in M_D$, then $Q_D = \emptyset$.

(iii) In step (iii), we establish the set E_D. By part (ii) of Proposition 4.4, E_D is a finite set and Corollary 4.3 states that $Q_D \neq \emptyset$ if and only if $E_D \neq \emptyset$.

(iv) Let $E_D \neq \emptyset$ and let $\#E_D = n$. In this step, we assign to each $[X_0, Y_0, \xi_0, \eta_0, e] \in E_D$ the polynomial

$$g(x) = x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}.$$

In this way, we obtain the full system of representatives $G_D = \{g_1(x), \dots, g_n(x)\}$ of $Q_D/{\sim}$. By part (iii) of Proposition 4.4, $Q_D/{\sim}$ is a finite set.

(v) Finally, applying Corollary 2.3 to each $g_i(x) \in G_D$, $i \in \{1, \dots, n\}$, we obtain the n sets $\{f_{i,w}(x); w \in \mathbb{Z}\}$ where

$$f_{i,w}(x) = x^4 + \frac{g_i'''(w)}{3!}x^3 + \frac{g_i''(w)}{2!}x^2 + \frac{g_i'(w)}{1!}x + g_i(w).$$

Hence, we get

$$Q_D = \bigcup_{i=1}^{n} \{f_{i,w}(x); w \in \mathbb{Z}\}.$$

The below example illustrates our method.

***Example* 4.6.** Let $D = -87$. Then we have

$$M_{-87} = \{[-320, \pm 11008], [-92, \pm 12376], [448, \pm 15616]\}.$$

Hence,

$$E_{-87}(-320, 11008) = \{[-80, \pm 1216], [-48, \pm 1728], [240, \pm 5184], [384, \pm 8640], [8592, \pm 796608]\},$$

$$E_{-87}(-320, -11008) = \emptyset,$$

$$E_{-87}(-92, 12376) = \{[-156, 0]\},$$

$$E_{-87}(-92, -12376) = \{[156, 0]\},$$

$$E_{-87}(448, 15616) = \{[-156, \pm 3240], [96, \pm 1728]\},$$

$$E_{-87}(448, -15616) = \emptyset.$$

Further, we have

$$E_{-87} = \big\{[-320, 11008, 240, 5184, 2], [-320, 11008, 240, -5184, 2],$$
$$[448, 15616, -156, -3240, 1], [448, 15616, -156, 3240, 3]\big\}.$$

Hence, it follows that $\#E_{-87} = \#Q_{-87}/{\sim} = 4$ and that $G_{-87} = \{g_1(x), g_2(x), g_3(x), g_4(x)\}$ where

$$g_1(x) = x^4 + 2x^3 - x^2 + x, \qquad g_2(x) = x^4 + 2x^3 - x^2 - 5x - 3,$$
$$g_3(x) = x^4 + x^3 + 2x^2 - x, \qquad g_4(x) = x^4 + 3x^3 + 5x^2 + 6x + 3.$$

Finally,

$$f_{1,w}(x) = x^4 + (4w+2)x^3 + (6w^2 + 6w - 1)x^2 + (4w^3 + 6w^2 - 2w + 1)x + w^4 + 2w^3 - w^2 + w,$$
$$f_{2,w}(x) = x^4 + (4w+2)x^3 + (6w^2 + 6w - 1)x^2 + (4w^3 + 6w^2 - 2w - 5)x + w^4 + 2w^3 - w^2 - 5w - 3,$$
$$f_{3,w}(x) = x^4 + (4w+1)x^3 + (6w^2 + 3w + 2)x^2 + (4w^3 + 3w^2 + 4w - 1)x + w^4 + w^3 + 2w^2 - w,$$
$$f_{4,w}(x) = x^4 + (4w+3)x^3 + (6w^2 + 9w + 5)x^2 + (4w^3 + 9w^2 + 10w + 6)x + w^4 + 3w^3 + 5w^2 + 6w + 3,$$

and

$$Q_{-87} = \bigcup_{i=1}^{4} \{f_{i,w}(x); w \in \mathbb{Z}\}.$$

Applying the method, the validity of Theorem 4.7 can be verified.

Theorem 4.7. *Let $0 \neq D \in \mathbb{Z}$ and let $1 \leq |D| \leq 1000$. Then we have:*

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

$$\begin{aligned} D \in \big\{&5, 12, 20, 21, 32, 40, 45, 48, 49, 60, 77, 81, 85, 96, 104, 112, 117, 125, 140, 144, 148, 165,\\ &169, 189, 192, 216, 221, 224, 229, 252, 256, 257, 260, 272, 285, 288, 320, 321, 333, 357,\\ &361, 392, 400, 404, 432, 437, 468, 469, 473, 480, 488, 500, 512, 525, 528, 533, 544, 549,\\ &564, 572, 580, 592, 605, 621, 629, 656, 672, 697, 725, 729, 733, 761, 768, 785, 788, 792,\\ &816, 832, 837, 864, 892, 896, 900, 916, 957, 981, 985\big\}. \end{aligned}$$

(ii) *If $-1 \geq D \geq -1000$, then $Q_D \neq \emptyset$ if and only if*

$$\begin{aligned} D \in \big\{&-3, -16, -23, -27, -31, -44, -59, -76, -83, -87, -107, -108, -112, -135, -139,\\ &-140, -175, -176, -199, -211, -231, -236, -240, -247, -255, -256, -268, -275,\\ &-279, -283, -288, -304, -331, -332, -335, -351, -367, -400, -416, -428, -432,\\ &-448, -464, -475, -491, -500, -507, -527, -556, -560, -563, -575, -588, -608,\\ &-643, -671, -684, -688, -695, -731, -751, -783, -800, -816, -844, -848, -863,\\ &-864, -891, -931, -944, -959, -972, -976, -983\big\}. \end{aligned}$$

5. Structure of the set Q_D

In this section, we establish some results related to the structure of the set Q_D. For $e \in \{0, 1, 2, 3\}$, put $Q_D(e) = \{x^4 + ax^3 + bx^2 + cx + d \in Q_D; a \equiv e \pmod 4\}$. Then $Q_D(0)$, $Q_D(1)$, $Q_D(2)$, $Q_D(3)$ are pairwise disjoint sets, and

$$Q_D = \bigcup_{e=0}^{4} Q_D(e).$$

Proposition 5.1 gives the important link between the sets $Q_D(1)$ and $Q_D(3)$.

Proposition 5.1. *Let $0 \neq D \in \mathbb{Z}$ and let $e \in \{1, 3\}$. Then there exists a one-to-one correspondence between the sets $Q_D(1)$ and $Q_D(3)$ given by the relation*

$$[X_0, Y_0, \xi_0, \eta_0, 1] \in E_D \Longleftrightarrow [X_0, Y_0, \xi_0, -\eta_0, 3] \in E_D.$$

Consequently, $Q_D(1) \neq \emptyset$ if and only if $Q_D(3) \neq \emptyset$.

Proof. First observe that $[\xi_0, \eta_0] \in E_D(X_0, Y_0)$ if and only if $[\xi_0, -\eta_0] \in E_D(X_0, Y_0)$.

If $e \in \{1, 3\}$, then, by (4.3), $\xi_0 \equiv 36 \pmod{96}$, which is equivalent to

$$18\xi_0 \equiv 648 \pmod{1728}. \tag{5.1}$$

Next, if $e = 1$, then, by (4.4), $9\xi_0 - \eta_0 - 108 \equiv 0 \pmod{1728}$. Using (5.1), this congruence can be written in the equivalent form

$$1719\xi_0 + \eta_0 + 108 \equiv 27\xi_0 + 94 \cdot 18\xi_0 + \eta_0 + 108 \equiv 27\xi_0 + \eta_0 + 540 \equiv 0 \pmod{1728}.$$

Hence, $[\xi_0, \eta_0]$ satisfies (4.4) for $e = 1$ if and only if $[\xi_0, -\eta_0]$ satisfies (4.4) for $e = 3$.

Furthermore, if $e \in \{1, 3\}$, then, by (4.3), $\xi_0 \equiv 36 \pmod{96}$, which is equivalent to

$$1152\xi_0 - 41472 \equiv 0 \pmod{110592}. \tag{5.2}$$

Next, if $e = 1$ then, from (4.4), it follows that $\eta_0 \equiv 9\xi_0 - 108 \pmod{1728}$ if and only if

$$576\xi_0 - 64\eta_0 - 6912 \equiv 0 \pmod{110592}. \tag{5.3}$$

Subtracting (5.3) from (5.2), we now obtain

$$576\xi_0 + 64\eta_0 - 34560 \equiv 0 \pmod{110592}. \tag{5.4}$$

Finally, if $e = 1$, then (4.5) yields

$$432 - \xi_0^2 - 72\xi_0 + 16\eta_0 + 144X_0 \equiv 0 \pmod{110592}. \tag{5.5}$$

Subtracting (5.4) from (5.5), we obtain

$$34992 - \xi_0^2 - 648\xi_0 - 48\eta_0 + 144X_0 \equiv 0 \pmod{110592}.$$

This proves that $[X_0, Y_0, \xi_0, \eta_0, 1] \in E_D$ if and only if $[X_0, Y_0, \xi_0, -\eta_0, 3] \in E_D$, which implies $Q_D(1) \neq \emptyset$ if and only if $Q_D(3) \neq \emptyset$. □

For the remaining cases $e \in \{0, 2\}$, we can prove Proposition 5.2.

Proposition 5.2. *Let $0 \neq D \in \mathbb{Z}$ and let $e \in \{0, 2\}$. Then we have:*

(i) $[X_0, Y_0, \xi_0, \eta_0, 0] \in E_D \iff [X_0, Y_0, \xi_0, -\eta_0, 0] \in E_D$.

(ii) $[X_0, Y_0, \xi_0, \eta_0, 2] \in E_D \iff [X_0, Y_0, \xi_0, -\eta_0, 2] \in E_D$.

Proof. Since part (i) of Proposition 5.2 immediately follows from (4.3)–(4.5), we prove (ii). Let $[X_0, Y_0, \xi_0, \eta_0, 2] \in E_D$. Then (4.3)–(4.5) yields that $\xi_0 \equiv 48 \pmod{96}$, $\eta_0 \equiv 18\xi_0 - 864 \pmod{1728}$, and

$$6912 - \xi_0^2 - 288\xi_0 + 32\eta_0 + 144X_0 \equiv 0 \pmod{110592}. \tag{5.6}$$

Since $\xi_0 \equiv 48 \pmod{96}$ is equivalent to $18\xi_0 \equiv 864 \pmod{1728}$, we have $-\eta_0 \equiv -18\xi_0 + 864 \equiv 1710\xi_0 - 864 = 18\xi_0 - 864 + 94 \cdot 18\xi_0 \equiv 18\xi_0 - 864 + 47 \cdot 1728 \equiv 18\xi_0 - 864 \pmod{1728}$. Further, $\xi_0 \equiv 48 \pmod{96}$ is equivalent to $1152\xi_0 \equiv 55296 \pmod{110592}$ and $\eta_0 \equiv 18\xi_0 - 864 \pmod{1728}$ is equivalent to $64\eta_0 \equiv 1152\xi_0 - 55296 \pmod{110592}$. Hence, we obtain $64\eta_0 \equiv 0 \pmod{110592}$ and $32\eta_0 \equiv -32\eta_0 \pmod{110592}$ follows. Now we see that (5.6) is equivalent to $6912 - \xi_0^2 - 288\xi_0 - 32\eta_0 + 144X_0 \equiv 0 \pmod{110592}$. This proves (ii). □

Remark 5.3. If $Q_D \neq \emptyset$, then any of the below seven cases can occur:

(i) $Q_D(0) \neq \emptyset$, $Q_D(1) \cup Q_D(3) \neq \emptyset$, $Q_D(2) \neq \emptyset$, $D = -23$,

(ii) $Q_D(0) \neq \emptyset$, $Q_D(1) \cup Q_D(3) \neq \emptyset$, $Q_D(2) = \emptyset$, $D = 32$,

(iii) $Q_D(0) \neq \emptyset$, $Q_D(1) \cup Q_D(3) = \emptyset$, $Q_D(2) \neq \emptyset$, $D = 5$,

(iv) $Q_D(0) = \emptyset$, $Q_D(1) \cup Q_D(3) \neq \emptyset$, $Q_D(2) \neq \emptyset$, $D = -87$,

(v) $Q_D(0) \neq \emptyset$, $Q_D(1) \cup Q_D(3) = \emptyset$, $Q_D(2) = \emptyset$, $D = -27$,

(vi) $Q_D(0) = \emptyset$, $Q_D(1) \cup Q_D(3) \neq \emptyset$, $Q_D(2) = \emptyset$, $D = 12$,

(vii) $Q_D(0) = \emptyset$, $Q_D(1) \cup Q_D(3) = \emptyset$, $Q_D(2) \neq \emptyset$, $D = -3$.

The above values of D are the least, in absolute value, for which the case occurs.

6. Even and odd solutions of Mordell's equation $Y^2 = X^3 - 2^{16}3^3D$

Some basic arithmetic properties of integer solutions $[X_0, Y_0]$ of the Mordell's equation $Y^2 = X^3 - 2^{16}3^3D$ have already been presented in Lemma 3.3. Combining part (i) and (ii) of Lemma 3.3, we immediately get $X_0 \equiv 0 \pmod 2 \iff Y_0 \equiv 0 \pmod 2$. 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

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

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

$$\varepsilon_{-1000} = 1572, \quad \varepsilon_{1000} = 1090, \quad o_{-1000} = 100, \quad \text{and} \quad o_{1000} = 44.$$

Hence, it follows that there exist approximately 95% even and only 5% odd integer solutions of $Y^2 = X^3 - 2^{16}3^3D$ for $0 \neq |D| \leq 1000$. This surprising fact inspires the study of even solutions in detail. As the main result of this section, we prove that, for any even solution $[X_0, Y_0]$, equation (4.2) can be replaced by another elliptic equation whose integer coefficients are substantially smaller in the absolute value than in (4.2).

We begin by recalling the well-known proposition concerning the solubility of linear congruences. See, for example, Hardy and Wright [4: p. 62, Theorem 57].

Proposition 6.1. *Let $a, b, m \in \mathbb{Z}$, $m > 1$ and let $g = \gcd(a, m)$. Then the congruence $ax \equiv b \pmod m$ is soluble if and only if $g|b$.*

Using Proposition 6.1, we now prove Lemma 6.2.

Lemma 6.2. *If $X_0, Y_0 \in \mathbb{Z}$, then the congruence $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ holds for at most one $\alpha \in \{0, 1, 2\}$.*

Proof. The proof consists of three steps. (i) First, suppose that $Y_0 \equiv 0 \pmod{27}$ and $3X_0 + Y_0 - 4 \equiv 0 \pmod{27}$. Then $Y_0 \equiv 4 - 3X_0 \equiv 0 \pmod{27}$, which yields $3X_0 \equiv 4 \pmod{27}$. Hence, $\gcd(3, 27) = 3 \nmid 4$, which is a contradiction.

(ii) Further, suppose that $Y_0 \equiv 0 \pmod{27}$ and $6X_0 + Y_0 - 32 \equiv 0 \pmod{27}$. Then $Y_0 \equiv 5 - 6X_0 \equiv 0 \pmod{27}$, which yields $6X_0 \equiv 5 \pmod{27}$. Hence, $\gcd(6, 27) = 3 \nmid 5$, which is a contradiction.

(iii) Finally, suppose that $3X_0 + Y_0 - 4 \equiv 0 \pmod{27}$ and $6X_0 + Y_0 - 32 \equiv 0 \pmod{27}$. Then $Y_0 \equiv 4 - 3X_0 \equiv 5 - 6X_0 \pmod{27}$, which yields $3X_0 \equiv 1 \pmod{27}$. Hence, $\gcd(3, 27) = 3 \nmid 1$, which is a contradiction. Combining (i)–(iii) proves the lemma. □

We are now ready to prove the main result of this section.

Theorem 6.3. *Let $0 \neq D \in \mathbb{Z}$ and let $[X_0, Y_0] \in \mathcal{E}_D$.*

(i) *If $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ does not hold for any $\alpha \in \{0, 1, 2\}$, then the system*

$$R^2 + 3T = X_0 \quad \textit{and} \quad R^3 - 9RT + 108S^2 = Y_0 \tag{6.1}$$

is not solvable in integers.

(ii) *If $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ holds for some $\alpha \in \{0, 1, 2\}$, then α is uniquely determined, $X_0 - 4\alpha^2 \equiv 0 \pmod{12}$, $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}$ and the set K of all integer solutions of (6.1) can be obtained from the set L of all integer solutions of the elliptic equation*

$$\eta^2 = \xi^3 - \alpha\xi^2 - \frac{X_0 - 4\alpha^2}{12}\xi + \frac{3\alpha X_0 + Y_0 - 4\alpha^3}{108}. \tag{6.2}$$

Moreover, between K and L, there exists a one-to-one correspondence.

Proof. (i) Let $[R_0, S_0, T_0]$ be an arbitrary integer solution of (6.1). Since $R_0 \in \mathbb{Z}$, there exits a uniquely determined $r \in \mathbb{Z}$ and $\alpha \in \{0, 1, 2\}$ such that $R_0 = 3r + \alpha$.

First, we prove

$$\frac{X_0 - 4\alpha^2}{12} \in \mathbb{Z} \iff 2|X_0. \tag{6.3}$$

Let $2|X_0$. Then, by part (i) of Lemma 3.3, $4|X_0$, and thus $4|X_0 - 4\alpha^2$. Next, the first equation in (6.1) yields $X_0 - R_0^2 \equiv X_0 - \alpha^2 \equiv 0 \pmod 3$, and $3|X_0 - 4\alpha^2$ follows. Hence, $12|X_0 - 4\alpha^2$, which means $(X_0 - 4\alpha^2)/12 \in \mathbb{Z}$. Because the validity of the converse implication is evident, we get (6.3).

Further, substituting $3T_0 = X_0 - R_0^2$ into $R_0^3 - 9R_0T_0 + 108S_0^2 = Y_0$, we obtain

$$4R_0^3 - 3X_0R_0 + 108S_0^2 = Y_0. \tag{6.4}$$

Since $R_0 = 3r + \alpha$, (6.4) can be written in the equivalent form

$$108S_0^2 = -108r^3 - 108\alpha r^2 + 9(X_0 - 4\alpha^2)r + 3\alpha X_0 + Y_0 - 4\alpha^3. \tag{6.5}$$

Reducing (6.5) by the modulus 108, using (6.3), we get $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}$. This proves (i).

(ii) Assume that there exists an $\alpha \in \{0, 1, 2\}$ such that $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$. Then Lemma 6.2 states that α is uniquely determined. Since $[X_0, Y_0] \in \mathcal{E}_D$, by part (i) of Lemma 3.3, $4|X_0$ and $8|Y_0$, which yields $4|3\alpha X_0 + Y_0 - 4\alpha^3$ for any $\alpha \in \{0, 1, 2\}$. Hence,

$$3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27} \iff 3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}.$$

We now prove that

$$3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27} \implies X_0 - 4\alpha^2 \equiv 0 \pmod{12}. \tag{6.6}$$

First, by part (i) of Lemma 3.3, $X_0 - 4\alpha^2 \equiv 0 \pmod 4$. Next, from the assumption $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$, we get $Y_0 \equiv \alpha^3 \equiv \alpha \pmod 3$. Hence, $Y_0^2 \equiv \alpha^2 \pmod 3$. Furthermore, it is clear from $[X_0, Y_0] \in \mathcal{E}_D$ that $Y_0^2 \equiv X_0^3 \pmod 3$, which, together with $X_0^3 \equiv X_0 \pmod 3$, yields $X_0 \equiv \alpha^2 \pmod 3$. Hence, $X_0 - 4\alpha^2 \equiv 0 \pmod 3$, and (6.6) follows.

Let $[R_0, S_0, T_0] \in K$. Then there exist a uniquely determined $r \in \mathbb{Z}$ and an $\alpha \in \{0, 1, 2\}$ such that $R_0 = 3r + \alpha$. In much the same way as in the proof of part (i), we get (6.5). Hence,

$$S_0^2 = -r^3 - \alpha r^2 + \frac{X_0 - 4\alpha^2}{12}r + \frac{3\alpha X_0 + Y_0 - 4\alpha^3}{108} \tag{6.7}$$

where $(X_0 - 4\alpha^2)/12$ and $(3\alpha X_0 + Y_0 - 4\alpha^3)/108$ are integers. Put $[\xi_0, \eta_0] = [-r, S_0]$. Then it follows from (6.7) that $[\xi_0, \eta_0] \in L$.

Conversely, let $[\xi_0, \eta_0] \in L$ where $\alpha \in \{0, 1, 2\}$ satisfies $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$. Put $R_0 = -3\xi_0 + \alpha$ and $S_0 = \eta_0$. Then $R_0, S_0 \in \mathbb{Z}$, and substituting $\xi_0 = (\alpha - R_0)/3$, $\eta_0 = S_0$ into (6.2) some calculation will yield

$$R_0^3 + 3R_0(R_0^2 - X_0) + 108S_0^2 = Y_0. \tag{6.8}$$

Next, put $T_0 = (X_0 - R_0^2)/3$. Since $R_0 = -3\xi_0 + \alpha$, we have $T_0 = 2\alpha\xi_0 - 3\xi_0^2 + (X_0 - \alpha^2)/3$, and by (6.6), $T_0 \in \mathbb{Z}$. Substituting $R_0^2 - X_0 = -3T_0$ into (6.8), we obtain $R_0^3 - 9R_0T_0 + 108S_0^2 = Y_0$. This proves that $[R_0, S_0, T_0] = [-3\xi_0 + \alpha, \eta_0, 2\alpha\xi_0 - 3\xi_0^2 + (X_0 - \alpha^2)/3] \in K$.

Moreover, it is evident that the mapping $\psi \colon L \to K$ defined by

$$\psi(\xi_0, \eta_0) = [-3\xi_0 + \alpha, \eta_0, 2\alpha\xi_0 - 3\xi_0^2 + (X_0 - \alpha^2)/3] \tag{6.9}$$

is bijective. The proof is complete. □

***Example* 6.4.** Let $D = -87$. Then $[X_0, Y_0] = [-320, 11008] \in \mathcal{E}_{-87}$, and for $\alpha = 1$, we have $3\alpha X_0 + Y_0 - 4\alpha^3 = 10044 \equiv 0 \pmod{27}$. By Theorem 6.3, the set K of all integer solutions of the system $R^2 + 3T = -320$ and $R^3 - 9RT + 108S^2 = 11008$ can be obtained using the set L of all integer solutions of the elliptic equation $\eta^2 = \xi^3 - \xi^2 + 27\xi + 93$. Since $L = \{[-1, \pm 8], [7, \pm 24], [11, \pm 40], [239, \pm 3688]\}$, (6.9) yields

$$K = \{[4, \pm 8, -112], [-20, \pm 24, -240], [-32, \pm 40, -448], [-716, \pm 3688, -170992]\}.$$

On the other hand, by Section 4, the set K can also be determined by means of the set $E_{-87}(-320, 11008) = \{[-80, \pm 1216], [-48, \pm 1728], [240, \pm 5184], [384, \pm 8640], [8592, \pm 796608]\}$ of all integer solutions of the elliptic equation $\eta^2 = \xi^3 + 34560\xi + 4755456$.

Remark 6.5. If $[X_0, Y_0] \in \mathcal{O}_D$, then $X_0 - 4\alpha^2 \not\equiv 0 \pmod{12}$ for any $\alpha \in \{0, 1, 2\}$. On the other hand, by examples, it can be proved that both cases (i) and (ii) can occur:

$$\text{(i) } 3\alpha X_0 + Y_0 - 4\alpha^3 \not\equiv 0 \pmod{108}, \qquad \text{(ii) } 3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}.$$

(i) If $D = -23$, then $[X_0, Y_0] = [489, 12555] \in \mathcal{O}_{-23}$, and for any $\alpha \in \{0, 1, 2\}$, we have $3\alpha X_0 + Y_0 - 4\alpha^3 \not\equiv 0 \pmod{108}$.

(ii) If $D = -107$, then $[X_0, Y_0] = [9241, 888445] \in \mathcal{O}_{107}$, and for $\alpha = 1$, we get $3\alpha X_0 + Y_0 - 4\alpha^3 = 916164 \equiv 0 \pmod{108}$.

7. Some conjectures related to Mordell's equation

Let $0 \neq D \in \mathbb{Z}$ and let

$$\mu_D = \begin{cases} 0 & \text{if } M_D = \emptyset, \\ 1 & \text{if } M_D \neq \emptyset. \end{cases}$$

Next, for any positive integer n, put

$$\sigma_n = \sum_{D=1}^{n} \mu_D \quad \text{and} \quad \sigma_{-n} = \sum_{D=-1}^{-n} \mu_D.$$

Computer investigation of the values σ_n and σ_{-n} for $n \leq 1000$ yields

$$\frac{\sigma_{1000}}{1000} = \frac{280}{1000} = 0.280, \quad \frac{\sigma_{-1000}}{1000} = \frac{426}{1000} = 0.426, \quad \frac{\sigma_{\ 1000}}{\sigma_{-1000}} = \frac{280}{426} \approx 0.657.$$

Hence, the following conjectures can be made:

$$\lim_{n\to\infty} \frac{\sigma_n}{n} = \frac{2}{7} \approx 0.286, \quad \lim_{n\to\infty} \frac{\sigma_{-n}}{n} = \frac{3}{7} \approx 0.429, \quad \lim_{n\to\infty} \frac{\sigma_n}{\sigma_{-n}} = \frac{2}{3} \approx 0.667. \tag{7.1}$$

The conjectures (7.1) lead to another interesting question, namely, whether some similar hypotheses can also be stated for the case of general Mordell's equation. It is clear that, to formulate such hypotheses, much computation will be needed.

Thanks to the computations made by M. A. Bennett and A. Ghadermarzi [1], all integer solutions of $Y^2 = X^3 + k$ are determined for any $0 \neq |k| \leq 10^7$. Based on their results, some new conjectures can be formulated. The following notations will be useful.

For $0 \neq k \in \mathbb{Z}$, let $M(k)$ denote the set of all integer solutions of $Y^2 = X^3 + k$, and let

$$\mu(k) = \begin{cases} 0 & \text{if } M(k) = \emptyset, \\ 1 & \text{if } M(k) \neq \emptyset. \end{cases}$$

Next, for any positive integer n, put

$$\sigma(n) = \sum_{k=1}^{n} \mu(k) \quad \text{and} \quad \sigma(-n) = \sum_{k=-1}^{n} \mu(-k).$$

By inspecting Table 1 and Table 2 in [1: pp. 642–643], we get

$$\frac{\sigma(10^7)}{10^7} = \frac{1332934}{10^7} \approx 0.133, \quad \frac{\sigma(-10^7)}{10^7} = \frac{834604}{10^7} \approx 0.083, \quad \frac{\sigma(-10^7)}{\sigma(10^7)} = \frac{834604}{1332934} \approx 0.626.$$

Hence, the following conjectures can be made:

$$\lim_{n\to\infty} \frac{\sigma(n)}{n} = \frac{2}{15} = 0.1\overline{3}, \quad \lim_{n\to\infty} \frac{\sigma(-n)}{n} = \frac{1}{12} = 0.08\overline{3}, \quad \lim_{n\to\infty} \frac{\sigma(-n)}{\sigma(n)} = \frac{5}{8} = 0.625. \qquad (7.2)$$

Our surmises can be proposed to the reader as Problem 7.1.

Problem 7.1. Prove or disprove (7.1) and (7.2).

8. Conclusion

The results presented in this paper make it possible to determine the set Q_D of all monic quartic polynomials $x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ with a given discriminant $0 \neq D \in \mathbb{Z}$. That provides an opportunity to study the following problem: Establish a general method of deciding in a finite number of steps whether, for a given $0 \neq D \in \mathbb{Z}$, the following statement holds: *Let p be an arbitrary prime. Then all polynomials in Q_D have the same type of factorization over the Galois field $\mathbb{F}_p$.* The validity of an analogous statement for the case of cubic polynomials has been recently examined in [10]–[15] with relatively closed results obtained.

Acknowledgement. The author thanks the anonymous referee for carefully reading the manuscript.

REFERENCES

[1] BENNETT, M. A.—GHADERMARZI, A.: *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18.1** (2015), 633–646.

[2] DICKSON, L. E.: *History of the Theory of Numbers*, Vol. II, Chelsea, New York, 1952.

[3] EVERTSE, J. H.—GYÖRY, K.: *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2017.

[4] HARDY, G. H.—WRIGHT, E. M.: *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, New York, 2008.

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

[6] GAUTHIER, S.—LÊ, F.: *On the youthful writings of Louis J. Mordell on the Diophantine equation $y^2 - k = x^3$*, Archive for History of Exact Sciences **73** (2019), 427–468.

[7] GEBEL, J.—PETHÖ, A.—ZIMMER, G. H.: *On Mordell's equation*, Compos. Math. **110** (1998), 335–367.

[8] GYÖRY, K.: *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426.

[9] GYÖRY, K.: *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69**(4) (2006), 473–499.

[10] KLAŠKA, J.—SKULA, L.: *Mordell's equation and the Tribonacci family*, Fibonacci Quart. **49**(4) (2011), 310–319.

[11] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the real case*, Util. Math. **102** (2017), 39–50.

[12] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Util. Math. **103** (2017), 99–109.

[13] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66**(4) (2016), 1019–1027.

[14] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the case of primes* 2 *and* 3, Math. Slovaca **67**(1) (2017), 71–82.

[15] KLAŠKA, J.—SKULA, L.: *On the factorizations of cubic polynomials with the same discriminant modulo a prime*, Math. Slovaca **68**(5) (2018), 987–1000.

[16] LONDON, J.—FINKELSTEIN, M.: *On Mordell's Equation* $y^2 - k = x^3$, Bowling Green, Ohio Bowling Green State University, 1973.

[17] MORDELL, L. J.: *A statement by Fermat*, Proc. Lond. Math. Soc. (2) **18** (1920), pp. v–vi.

[18] SIEGEL, C. L.: *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss Akad. Wiss., 1929, pp. 1–41.

[19] SMART, N. P.: *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1998.

Received 16. 11. 2020
Accepted 25. 1. 2021

Institute of Mathematics
Faculty of Mechanical Engineering
Brno University of Technology
Technická 2
616 69 Brno
CZECH REPUBLIC
E-mail: klaska@fme.vutbr.cz