The group of integer solutions of the Diophantine equation $x^2 + mxy + ny^2 = 1$

Ghader Ghasemi
Department of Mathematics
Faculty of Sciences
University of Mohaghegh Ardabili
56199-11367, Ardabil
Iran
ghasemi@uma.ac.ir

Abstract. Let m and n be two integers. It is shown that the set of all integer solutions of the Diophantine equation $x^2 + mxy + ny^2 = 1$ has an Abelian group structure. Furthermore, it is shown that this Abelian group is isomorphic to one of the groups $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}$.

Keywords: Abelian group, commutative ring, Diophantine equation, Pell's equation, torsion subgroup.

1. Introduction

In mathematics, a Diophantine equation is a polynomial equation, usually involving two or more unknowns, such that the only solutions of interest are the integer ones (an integer solution is such that all the unknowns take integer values).

Recall that an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation $y^2 = x^3 + ax + b$, along with a distinguished point at infinity. The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3. This set together with the group operation of elliptic curves is an Abelian group, with the point at infinity as an identity element.

Pursuing this point of view further, in this paper we focused on the set of the points satisfying the equation $x^2 + \eta xy + \xi y^2 = 1_R$, where the coordinates are to be chosen from a commutative ring R with the identity element 1_R. We prove that this set together with a suitable group operation is an Abelian group, with $e = (1_R, 0_R)$ as the identity element. Also, by using this result we study the set of all integer solutions of the Diophantine equation $x^2 + mxy + ny^2 = 1$, where $m, n \in \mathbb{Z}$. Recall that one special case of these equations is the *Pell's equation*, which has a historical background.

We prove that in general the Abelian group of all integer solutions of the Diophantine equation $x^2 + mxy + ny^2 = 1$ is isomorphic to one of the groups

$\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}$. Also, we show that the set of all integer solutions of the *Pell's equation* as an Abelian group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.

Throughout this paper, for each element g of a given group $(G, *)$ we denote the order of g by $o(g)$. Also, for each subgroup H of G we denote the order of H by $|H|$. For any unexplained notation and terminology, we refer to [1] and [2].

2. The results

We start this section with the following theorem.

Theorem 2.1. *Let $(R, +, \cdot)$ be a commutative ring with the identity element 1_R and η, ξ be two arbitrary elements of R. Set*

$$G(R, \eta, \xi) := \left\{(a, b) \in R \times R \ : \ a^2 + \eta ab + \xi b^2 = 1_R\right\}.$$

Define the binary operation $*$ on $G(R, \eta, \xi)$ as $(a, b) * (c, d) := (ac - \xi bd, bc + ad + \eta bd)$, for each $(a, b), (c, d) \in G(R, \eta, \xi)$. Then, $(G(R, \eta, \xi), *)$ is an Abelian group with the identity element $e = (1_R, 0_R)$ such that $(a, b)^{-1} = (a + \eta b, -b)$, for each $(a, b) \in G(R, \eta, \xi)$.

Proof. For each $g = (a, b)$, $g' = (c, d) \in G(R, \eta, \xi)$, by the definition we have

$$a^2 + \eta ab + \xi b^2 = 1_R = c^2 + \eta cd + \xi d^2.$$

Therefore,

$$\begin{aligned} 1_R &= (1_R)(1_R) \\ &= (a^2 + \eta ab + \xi b^2)(c^2 + \eta cd + \xi d^2) \\ &= (ac - \xi bd)^2 + \eta(ac - \xi bd)(bc + ad + \eta bd) + \xi(bc + ad + \eta bd)^2, \end{aligned}$$

which shows that $g * g' = (ac - \xi bd, bc + ad + \eta bd) \in G(R, \eta, \xi)$.

We show that $*$ is associative. For each $g = (a, b)$, $g' = (c, d)$, $g'' = (u, v) \in G(R, \eta, \xi)$, one sees that

$$\begin{aligned} (g * g') * g'' &= (ac - \xi bd, bc + ad + \eta bd) * (u, v) \\ &= (r, s) \\ &= (a, b) * (cu - \xi dv, du + cv + \eta dv) \\ &= g * (g' * g''), \end{aligned}$$

where

$$\begin{aligned} r &= (ac - \xi bd)u - \xi(bc + ad + \eta bd)v \\ &= acu - \xi bdu - \xi bcv - \xi adv - \xi \eta bdv \\ &= acu - \xi adv - \xi bdu - \xi bcv - \xi \eta bdv \\ &= a(cu - \xi dv) - \xi b(du + cv + \eta dv), \end{aligned}$$

and

$$\begin{aligned} s &= (bc+ad+\eta bd)u+(ac-\xi bd)v+\eta(bc+ad+\eta bd)v \\ &= bcu+adu+\eta bdu+acv-\xi bdv+\eta bcv+\eta adv+\eta^2 bdv \\ &= bcu-\xi bdv+adu+acv+\eta adv+\eta bdu+\eta bcv+\eta^2 bdv \\ &= b(cu-\xi dv)+a(du+cv+\eta dv)+\eta b(du+cv+\eta dv). \end{aligned}$$

Moreover, for each $g=(a,b)$, $g'=(c,d)\in G(R,\eta,\xi)$, it is clear that

$$g*g'=(ac-\xi bd, bc+ad+\eta bd)=(ca-\xi db, cb+da+\eta db)=g'*g.$$

Hence, the binary operation $*$ is commutative.

Also, for each $g=(a,b)\in G(R,\eta,\xi)$, we see that

$$e*g=g=g*e,$$

where $e=(1_R,0_R)$. So e is the identity element of $G(R,\eta,\xi)$ with respect to the binary operation $*$.

Let $g=(a,b)\in G(R,\eta,\xi)$ and put $h=(c,d):=(a+\eta b,-b)$. By the definition from the assumption $g=(a,b)\in G(R,\eta,\xi)$ it follows that $a^2+\eta ab+\xi b^2=1_R$, and so

$$\begin{aligned} c^2+\eta cd+\xi d^2 &= (a+\eta b)^2+\eta(-b)(a+\eta b)+\xi(-b)^2 \\ &= a^2+2\eta ab+\eta^2b^2-\eta ab-\eta^2b^2+\xi b^2 \\ &= a^2+\eta ab+\xi b^2=1_R. \end{aligned}$$

Therefore, $h=(c,d)\in G(R,\eta,\xi)$. Also, we have

$$ac-\xi bd=a(a+\eta b)-\xi b(-b)=a^2+\eta ab+\xi b^2=1_R,$$

and

$$bc+ad+\eta bd=b(a+\eta b)+a(-b)+\eta b(-b)=ab+\eta b^2-ab-\eta b^2=0_R.$$

Thus, $h=(c,d)=(a+\eta b,-b)$ is an element of $G(R,\eta,\xi)$ such that

$$h*g=g*h=(ac-\xi bd, bc+ad+\eta bd)=(1_R,0_R)=e.$$

Hence, every element $g=(a,b)\in G(R,\eta,\xi)$ has an inverse in $G(R,\eta,\xi)$ and $g^{-1}=(a+\eta b,-b)$

Now, we are ready to deduce that $(G(R,\eta,\xi),*)$ is an Abelian group with the identity element $e=(1_R,0_R)$. □

The following lemma is needed in the proof of Lemma 2.3.

Lemma 2.1. *Let $(R,+,\cdot)$ be a commutative ring with an identity element and η, ξ be two arbitrary elements of R. Then, for each $g=(a,b)\in G(R,\eta,\xi)$ and each integer $k\geq 2$, there are elements $u_k, v_k\in R$ such that*

$$g^k=(a^k+u_kb^2, kba^{k-1}+v_kb^2).$$

Proof. We use induction on k. Since for $k = 2$ we have

$$g^2 = g * g = (a^2 - \xi b^2, 2ab + \eta b^2),$$

it is clear that the elements $u_2 = -\xi$ and $v_2 = \eta$ satisfy the desired condition. Now, let $k > 2$ and assume that the result has been proved for $k - 1$. Then, by inductive assumption there are elements $u_{k-1}, v_{k-1} \in R$ such that

$$g^{k-1} = (a^{k-1} + u_{k-1}b^2, (k-1)ba^{k-2} + v_{k-1}b^2).$$

Therefore,

$$\begin{aligned} g^k &= g * g^{k-1} \\ &= (a, b) * (a^{k-1} + u_{k-1}b^2, (k-1)ba^{k-2} + v_{k-1}b^2) \\ &= (a^k + u_k b^2, kba^{k-1} + v_k b^2), \end{aligned}$$

where

$$u_k = au_{k-1} - \xi bv_{k-1} - \xi(k-1)a^{k-2}, \text{ and } v_k = bu_{k-1} + (a+\eta b)v_{k-1} + \eta(k-1)a^{k-2}.$$

This completes the inductive step. □

In the sequel for each pair of integers m and n let $(\mathfrak{B}_{m,n}, *)$ denote the Abelian group $(G(\mathbb{Z}, m, n), *)$. The remainder of this section will be devoted to a discussion about the basic properties of the Abelian groups $(\mathfrak{B}_{m,n}, *)$, where $m, n \in \mathbb{Z}$.

Lemma 2.2. *Let m and n be two integers. Then, the following statements hold:*

i) *Suppose that $g = (a, b) \in \mathfrak{B}_{m,n}$. Then, $o(g) = 2$ if and only if $g = (-1, 0)$.*

ii) *Assume that $g = (a, b) \in \mathfrak{B}_{m,n}$ is an element of finite order k for some $k \geq 3$. Then, b divides k.*

iii) *Let p be a prime integer. If there is an element $g = (a, b) \in \mathfrak{B}_{m,n}$ of order p, then either $p = 2$ or $p = 3$.*

Proof. (i) If $o(g) = 2$, then it is clear that $(a, b) = g = g^{-1} = (a + mb, -b)$. Hence, $b = 0$ and $g = (a, 0)$. Since

$$(1, 0) = e = g^2 = (a, 0) * (a, 0) = (a^2, 0),$$

we see that $a = \pm 1$. Also, from the hypothesis $o(g) = 2$, we get $g \neq (1, 0)$, which implies that $a = -1$ and $g = (-1, 0)$. Conversely, if $g = (-1, 0) \in \mathfrak{B}_{m,n}$, then we see that $o(g) = 2$. Thus, $o(g) = 2$ if and only if $g = (-1, 0)$.

(ii) We claim that $b \neq 0$. Assume the opposite. Then, $g = (a, 0)$ and so

$$(1, 0) = e = g^k = (a^k, 0).$$

Hence, $a = \pm 1$ and so $g = e$ or $g = (-1, 0)$. Thus, $g^2 = e$ and so $k = o(g) \leq 2$, which is a contradiction. By the definition we have $g^k = e = (1, 0)$ and by Lemma 2.2 there are elements $u, v \in \mathbb{Z}$ such that

$$g^k = (a^k + ub^2, kba^{k-1} + vb^2).$$

Therefore, $kba^{k-1}+vb^2 = 0$. Since $a^2+mab+nb^2 = 1$, it is clear that the integers a and b are relatively prime and so the integers a^{k-1} and b are relatively prime as well. Also, from the assumption $b \neq 0$ and the relation $kba^{k-1} + vb^2 = 0$, we can deduce that $ka^{k-1} = -vb$. Therefore, b divides k.

(iii) Assume the opposite. Then, there is a prime integer $p > 3$ such that $o(g) = p$ for some element $g = (a, b) \in \mathfrak{B}_{m,n}$. We claim that $b = \pm 1$. Assume the opposite. Then, we have $b \neq \pm 1$. By (ii) we know that b divides p. Since p is a prime integer and $b \neq \pm 1$, it is concluded that $b = \pm p$. Furthermore, by Lemma 2.2 there are integers u', v' such that

$$(1, 0) = e = g^p = (a^p + u'b^2, pba^{p-1} + v'b^2) = (a^p + p^2u', \pm p^2a^{p-1} + p^2v').$$

From the relation $a^p + p^2u' = 1$ it follows that a^p is congruent to 1 (mod p). Also, by *Fermat's Theorem* we know that a^p is congruent to a (mod p). Thus, a is congruent to 1 (mod p) and hence $2a$ is congruent to 2 (mod p). Furthermore, since p is an odd prime it can be seen that the following element

$$g^2 = (a^2 - nb^2, 2ab + mb^2) = (a^2 - p^2n, \pm 2pa + p^2m),$$

is of order p as well. Now, if $\pm 2pa + p^2m \neq \pm 1$ then by the same argument it follows that

$$\pm 2pa + p^2m = \pm p.$$

Consequently, $\pm 2a + mp = \pm 1$. Therefore, $2a$ is congruent to ± 1 (mod p). Thus, 2 is congruent to ± 1 (mod p). Hence, we must have $p = 3$, which is a contradiction. Therefore, $\pm 2pa + p^2m = \pm 1$. So, we have $p(\pm 2a + pm) = \pm 1$. Hence, $p = \pm 1$, which is a contradiction. Therefore, $g = (a, b) = (a, \pm 1)$ and $b^2 = 1$. Moreover, since the element $g^2 = (a^2 - nb^2, 2ab + mb^2) = (a^2 - n, 2ab + m) \in \mathfrak{B}_{m,n}$ is of order p, by the same argument we see that $2ab + m = \pm 1$. Hence, $ab = \frac{-1-m}{2}$ or $ab = \frac{1-m}{2}$. By using the assumption $b = \pm 1$, from these relations we obtain

$$(a, b) \in \left\{ (\frac{-1-m}{2}, 1), (\frac{1+m}{2}, -1), (\frac{1-m}{2}, 1), (\frac{-1+m}{2}, -1) \right\}.$$

Hence, there are at most four elements $g = (a, b)$ of order p in $\mathfrak{B}_{m,n}$. Clearly, all of the $p - 1$ distinct elements $g, g^2, ..., g^{p-1}$ are of order p. This observation shows that the only possible case is $p = 5$. Also, in this situation the set $\big\{(\frac{-1-m}{2}, 1), (\frac{1+m}{2}, -1), (\frac{1-m}{2}, 1), (\frac{-1+m}{2}, -1)\big\}$ is a subset of $\mathfrak{B}_{m,n}$ and all of its elements are of order p. Set $h = (u, v) := (\frac{-1-m}{2}, 1)$ and $t := (-1, 0)$. Then, we have $h, t \in \mathfrak{B}_{m,n}$ and $t * h = (\frac{1+m}{2}, -1)$. Therefore, $o(h) = o(t * h) = p$. Hence, $t^p = t^p * e = t^p * h^p = (t * h)^p = e$. Therefore, $o(t)$ divides p, which is a contradiction since $o(t) = 2$ and $p > 3$ is a prime integer. □

The following lemma and its corollary will be quite useful in this paper.

Lemma 2.3. *Let m and n be two integers. If H is a finite subgroup of $\mathfrak{B}_{m,n}$, then there are non-negative integers α and β such that $|H| = 2^{\alpha} \times 3^{\beta}$.*

Proof. Assume the opposite. Then, there is a prime integer $p > 3$ such that p divides $|H|$. So, in view of *Cauchy's Theorem*, (see [3]), the group H contains an element h of order p. But, by Lemma 2.3 this is a contradiction. □

Corollary 2.1. *Let m and n be two integers. If $g \in \mathfrak{B}_{m,n}$ is an element of finite order, then there are non-negative integers α and β such that $o(g) = 2^{\alpha} \times 3^{\beta}$.*

Proof. Let $H := \langle g \rangle$. Then, H is a subgroup of $\mathfrak{B}_{m,n}$ with $|H| = o(g) < \infty$. Now the assertion follows from Lemma 2.4. □

The following lemmas are of assistance in the proof of Theorem 2.14.

Lemma 2.4. *Let m and n be two integers. Then, each finite 2-subgroup of $\mathfrak{B}_{m,n}$ is cyclic.*

Proof. Assume the opposite. Then, there is a finite 2-subgroup H of $\mathfrak{B}_{m,n}$ such that H is not cyclic. Therefore, by the *Fundamental Theorem of Finite Abelian Groups* we have

$$H \simeq \prod_{i=1}^{k} \mathbb{Z}_{2^{\ell_i}},$$

for some positive integers $\ell_1 \leq \ell_2 \leq \cdots \leq \ell_k$ with the property $|H| = 2^{\ell_1+\ell_2+\cdots+\ell_k}$ and $k \geq 2$. Furthermore, in this situation H has a subgroup K such that

$$K \simeq \prod_{i=1}^{k} \mathbb{Z}_2.$$

Thus, K contains exactly $2^k - 1$ distinct elements of order 2. Since $k \geq 2$ it follows that $\mathfrak{B}_{m,n}$ contains at least 3 distinct elements of order 2. But, by Lemma 2.3 there is precisely one element $g = (a, b) \in \mathfrak{B}_{m,n}$ with $o(g) = 2$, which is a contradiction. □

Lemma 2.5. *Let m and n be two integers. Then, each finite 3-subgroup of $\mathfrak{B}_{m,n}$ is cyclic.*

Proof. Assume the opposite. Then, there is a finite 3-subgroup H of $\mathfrak{B}_{m,n}$ such that H is not cyclic. Therefore, by the *Fundamental Theorem of Finite Abelian Groups* we have

$$H \simeq \prod_{i=1}^{k} \mathbb{Z}_{3^{\ell_i}},$$

for some positive integers $\ell_1 \leq \ell_2 \leq \cdots \leq \ell_k$ with the property $|H| = 3^{\ell_1+\ell_2+\cdots+\ell_k}$ and $k \geq 2$. Furthermore, in this situation H has a subgroup K such that

$$K \simeq \prod_{i=1}^{k} \mathbb{Z}_3.$$

Thus, K contains exactly $3^k - 1$ distinct elements of order 3. Since $k \geq 2$ it follows that $\mathfrak{B}_{m,n}$ has at least 8 distinct elements of order 3. Assume that $g = (a, b) \in \mathfrak{B}_{m,n}$ is an element of order 3. Then, by Lemma 2.3 we know that b divides 3. Hence, $b \in \{\pm 1, \pm 3\}$. Moreover, from the relation $o(g) = 3$, we get $g^2 = g^{-1}$. Thus, $(a^2 - nb^2, 2ab + mb^2) = (a + mb, -b)$. So, $2ab + mb^2 = -b$, and by using the hypothesis $b \neq 0$, we obtain $a = \frac{-1-mb}{2}$. This observation shows that there are at most 4 distinct elements $g = (a, b) \in \mathfrak{B}_{m,n}$ with $o(g) = 3$, which is a contradiction. □

Lemma 2.6. *Let m and n be two integers. Then, each finite subgroup of $\mathfrak{B}_{m,n}$ is cyclic.*

Proof. Let H be a finite subgroup of $\mathfrak{B}_{m,n}$. Then, by Lemma 2.4 there are non-negative integers α and β such that $|H| = 2^\alpha \times 3^\beta$. Let P and Q denote the Sylow 2-subgroup and the Sylow 3-subgroup of H respectively. Then, by Lemmas 2.6 and 2.7, P and Q are cyclic groups. Therefore, from the relations $H = P \oplus Q$ and $(|P|, |Q|) = 1$, it is concluded that H is a cyclic group. □

Corollary 2.2. *Let $m, n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, $H_k := \{g \in \mathfrak{B}_{m,n} \ : \ g^k = e\}$ is a finite subgroup of $\mathfrak{B}_{m,n}$. In particular, $S_k := \{g \in \mathfrak{B}_{m,n} \ : \ o(g) = k\}$ is a finite set.*

Proof. Assume the opposite. Then, we can find a finite subgroup K of H_k with $|K| > k$. Therefore, by Lemma 2.8, K is a cyclic group. So, there exists an element $g \in K$ such that $K = \langle g \rangle$. By the hypothesis we have $g^k = e$ and hence $|K| = o(g) \leq k$, which is a contradiction. Since $S_k \subseteq H_k$, we see that S_k is a finite set as well. □

Lemma 2.7. *Let $m, n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, for each $b \in \mathbb{Z}$ there is at most one integer a such that $(a, b) \in \mathfrak{B}_{m,n}$ and $o((a, b)) = k$.*

Proof. Assume that $g = (a, b) \in \mathfrak{B}_{m,n}$ and $o(g) = k$. Then, by the definition we have

$$(1, 0) = g^k = (P(a, b, m, n), Q(a, b, m, n)),$$

for some polynomials $P(X_1, X_2, X_3, X_4), Q(X_1, X_2, X_3, X_4) \in \mathbb{Z}[X_1, X_2, X_3, X_4]$. Since $a^2 = 1 - mab - nb^2$, we can write $P(a, b, m, n) = H_1(b, m, n) + aH_2(b, m, n)$ and $Q(a, b, m, n) = H_3(b, m, n) + aH_4(b, m, n)$, for some $H_1(X_1, X_2, X_3)$, $H_2(X_1, X_2, X_3)$, $H_3(X_1, X_2, X_3)$, $H_4(X_1, X_2, X_3) \in \mathbb{Z}[X_1, X_2, X_3]$.

By Corollary 2.9, there are only a finite number of elements $g \in \mathfrak{B}_{m,n}$ with $o(g) = k$. Therefore, for each element $b \in \mathbb{Z}$, there are only a finite number of integers a such that $(a,b) \in \mathfrak{B}_{m,n}$ and $o((a,b)) = k$. This observation implies that for each $b \in \mathbb{Z}$, $H_2(b,m,n) \neq 0$ or $H_4(b,m,n) \neq 0$. So, we can find at most one integer a such that $H_1(b,m,n) + aH_2(b,m,n) = 1$ and $H_3(b,m,n) + aH_4(b,m,n) = 0$. Thus, for each $b \in \mathbb{Z}$, there is at most one integer a such that $(a,b) \in \mathfrak{B}_{m,n}$ and $o((a,b)) = k$. □

Let m and n be two integers. In the sequel, we will denote the torsion subgroup of $\mathfrak{B}_{m,n}$ by $\mathfrak{T}_{m,n}$. We recall that the torsion subgroup of $\mathfrak{B}_{m,n}$ is defined as:

$$\mathfrak{T}_{m,n} := \{g \in \mathfrak{B}_{m,n} \ : \ o(g) < \infty\}.$$

Lemma 2.8. *Let m and n be two integers. Then, the following statements hold:*

i) *Let $g_1 = (a_1, b_1) \in \mathfrak{T}_{m,n}$ be an element of order 4. Then, b_1 divides 2.*

ii) *Suppose that $g_2 = (a_2, b_2) \in \mathfrak{T}_{m,n}$ is an element of order 8. Then, b_2 divides 2.*

iii) *Assume that $g_3 = (a_3, b_3) \in \mathfrak{T}_{m,n}$ is an element of order 6. Then, b_3 divides 3.*

iv) *Let $g_4 = (a_4, b_4) \in \mathfrak{T}_{m,n}$ be an element of order 12. Then, b_4 divides 3.*

Proof. (i) By Lemma 2.3, b_1 divides 4 and so $b_1 \neq 0$. Since $o(g_1) = 4$, it is clear that $o(g_1^2) = 2$. Thus, by Lemma 2.3 we have $g_1^2 = (-1, 0)$. Hence, $(a_1^2 - nb_1^2, 2a_1b_1 + mb_1^2) = (-1, 0)$. So, from the relations $b_1 \neq 0$ and $b_1(2a_1 + mb_1) = 0$, it follows that $2a_1 + mb_1 = 0$. Since $a_1^2 + ma_1b_1 + nb_1^2 = 1$, it is clear that the integers a_1 and b_1 are relatively prime. Therefore, the relation $2a_1 = -mb_1$ shows that b_1 divides 2.

(ii) Since $o(g_2) = 8$, it is clear that $o(g_2^2) = 4$. Also, the relation $g_2^2 = (a_2^2 - nb_2^2, 2a_2b_2 + mb_2^2)$ together with (i) implies that $2a_2b_2 + mb_2^2$ divides 2. Since b_2 divides $2a_2b_2 + mb_2^2$, it follows that b_2 divides 2.

(iii) Since $o(g_3) = 6$, it follows that $o(g_3^3) = 2$. Thus, by Lemma 2.3 we have $g_3^3 = (-1, 0)$. Put $t := (-1, 0)$. Since $o(g_3) = 6$, it can be seen that

$$\begin{aligned}
(nb_3^2 - a_3^2, -2a_3b_3 - mb_3^2) &= t * g_3^2 \\
&= g_3^3 * g_3^2 \\
&= g_3^5 \\
&= g_3^{-1} \\
&= (a_3 + mb_3, -b_3),
\end{aligned}$$

which shows that $-2a_3b_3 - mb_3^2 = -b_3$. By Lemma 2.3, b_3 divides 6 and so $b_3 \neq 0$. Thus, $mb_3 = -2a_3 + 1$ and hence 2 doesn't divide b_3. Therefore, b_3 divides 3.

(iv) Since $o(g_4) = 12$, it is clear that $o(g_4^2) = 6$. Also, the relation $g_4^2 = (a_4^2 - nb_4^2, 2a_4b_4 + mb_4^2)$ together with (iii) implies that $2a_4b_4 + mb_4^2$ divides 3. Since b_4 divides $2a_4b_4 + mb_4^2$, it is concluded that b_4 divides 3. □

Lemma 2.9. *Let m and n be two integers. Then, the following statements hold:*

i) *Assume that $g \in \mathfrak{T}_{m,n}$ is an element of order 2^k for some $k \in \mathbb{N}_0$. Then, $k \leq 2$.*

ii) *Suppose that $h \in \mathfrak{T}_{m,n}$ is an element of order 3^k for some $k \in \mathbb{N}_0$. Then, $k \leq 2$.*

Proof. (i) Assume the opposite. Then, we have $o(g) = 2^k$ for some $k \geq 3$. Therefore, $o(g^{2^{k-3}}) = 8$. By replacing g with $g^{2^{k-3}}$, we may assume that $o(g) = 8$. Let $g_1 = (a, b) \in \mathfrak{T}_{m,n}$ be an element of order 8. Then, by Lemma 2.11 we see that b divides 2. Thus, $b \in \{\pm1, \pm2\}$. Since $o(g) = 8$, one sees that there are exactly 4 distinct elements of order 8 in the subgroup $\langle g\rangle$ of $\mathfrak{T}_{m,n}$. Thus, by Lemma 2.10 for each $b \in \{\pm1, \pm2\}$ there is a unique integer a such that $g_1 = (a, b) \in \langle g\rangle$ and $o(g_1) = 8$. Let $g_2 = (c, d)$ be an element of $\langle g\rangle$ with $o(g_2) = 4$. Then, by Lemma 2.11 we see that d divides 2. Hence, $d \in \{\pm1, \pm2\}$. So, there is a unique integer a such that $g_3 = (a, d) \in \langle g\rangle$ and $o(g_3) = 8$. From the relations $a^2 + mad + nd^2 = 1$ and $c^2 + mcd + nd^2 = 1$, we get $(a - c)(a + c + md) = 0$. Since $o(g_2) = 4$ and $o(g_3) = 8$, it follows that $g_2 \neq g_3$ and so $a \neq c$. Thus, from the relations $a - c \neq 0$ and $(a - c)(a + c + md) = 0$, it is concluded that $a + c + md = 0$. Therefore, $g_3^{-1} = (a + md, -d) = (-c, -d) = (-1, 0) * g_2$, which implies that $(g_3^{-1})^4 = (-1, 0)^4 * g_2^4 = e$. Hence, $8 = o(g_3) = o(g_3^{-1}) \leq 4$, which is a contradiction.

(ii) Assume the opposite. So, we have $o(h) = 3^k$ for some $k \geq 3$. Hence, $o(h^{3^{k-3}}) = 27$. By replacing h with $h^{3^{k-3}}$, we my assume that $o(h) = 27$. Let $h_1 = (r, s) \in \mathfrak{T}_{m,n}$ be an element of order 27. Then, by Lemma 2.3 we see that s divides 27. Hence, $s \in \{\pm1, \pm3, \pm9, \pm27\}$. Therefore, by Lemma 2.10 there are at most 8 elements $h_1 = (r, s) \in \mathfrak{T}_{m,n}$ with the property $o(h_1) = 27$. Since $o(h) = 27$, one sees that there are exactly 18 elements of order 27 in the subgroup $\langle h\rangle$ of $\mathfrak{T}_{m,n}$, which is a contradiction. □

Lemma 2.10. *Let m and n be two integers. Suppose that $h \in \mathfrak{T}_{m,n}$ is an element of order 3^k for some $k \in \mathbb{N}_0$. Then, $k \leq 1$.*

Proof. Assume the opposite. Since by Lemma 2.12 we have $k \leq 2$, it follows that $k = 2$. Let $h_1 = (a, b) \in \mathfrak{T}_{m,n}$ be an element of order 9. Then, by Lemma 2.3 we see that b divides 9. Hence, $b \in \{\pm1, \pm3, \pm9\}$. Since $o(h) = 9$, one sees that there are exactly 6 elements of order 9 in the subgroup $\langle h\rangle$ of $\mathfrak{T}_{m,n}$. Thus, by Lemma 2.10 for each $b \in \{\pm1, \pm3, \pm9\}$ there is a unique integer a such that $h_1 = (a, b) \in \langle h\rangle$ and $o(h_1) = 9$. Let $h_2 = (c, d)$ be an element of $\langle h\rangle$ with $o(h_2) = 3$. Then, by Lemma 2.3 we see that d divides 3. Hence, $d \in \{\pm1, \pm3\}$. So, there is a unique integer a such that $h_3 = (a, d) \in \langle h\rangle$ and $o(h_3) = 9$. From the relations $a^2 + mad + nd^2 = 1$ and $c^2 + mcd + nd^2 = 1$, we get $(a - c)(a + c + md) = 0$. Since $o(h_2) = 3$ and $o(h_3) = 9$, it follows that $h_2 \neq h_3$ and so $a \neq c$. Thus, from the relations $a - c \neq 0$ and $(a - c)(a + c + md) = 0$, it is concluded that $a + c + md = 0$. Therefore, $h_3^{-1} = (a + md, -d) = (-c, -d) = (-1, 0) * h_2$, which implies that $(h_3^{-1})^6 = (-1,0)^6 * h_2^6 = e$. Hence, $9 = o(h_3) = o(h_3^{-1}) \leq 6$, which is a contradiction. □

The following result plays a key role in the proof of our main theorem.

Theorem 2.2. *Let m and n be two integers. Then, the Abelian group $\mathfrak{T}_{m,n}$ is isomorphic to $\mathbb{Z}_k$ for some $k \in \{2,4,6\}$.*

Proof. We claim that $|\mathfrak{T}_{m,n}| \leq 12$. Assume the opposite. Then, we have $|\mathfrak{T}_{m,n}| > 12$. Therefore, we can find a finite subgroup H of $\mathfrak{T}_{m,n}$ with $|H| > 12$. By Lemma 2.8, H is a cyclic group. Thus, there is an element $g_1 \in H$ with $H = \langle g_1 \rangle$. In view of Corollary 2.5, there are integers $\alpha_1, \beta_1 \in \mathbb{N}_0$ such that $o(g_1) = 2^{\alpha_1} \times 3^{\beta_1}$. Since $2^{\alpha_1} \times 3^{\beta_1} = o(g_1) = |H| > 12 = 2^2 \times 3$, we can deduce that $\alpha_1 \geq 3$ or $\beta_1 \geq 2$. Moreover, it is clear that

$$o(g_1^{2^{\alpha_1}}) = 3^{\beta_1} \text{ and } o(g_1^{3^{\beta_1}}) = 2^{\alpha_1}.$$

Therefore, by Lemma 2.12 and Lemma 2.13 we get $\alpha_1 \leq 2$ and $\beta_1 \leq 1$, which is a contradiction. So, we have $|\mathfrak{T}_{m,n}| \leq 12$. Hence, by Lemma 2.8 it is concluded that $\mathfrak{T}_{m,n}$ is a cyclic subgroup of $\mathfrak{B}_{m,n}$. Therefore, there exists an element $g_2 \in \mathfrak{T}_{m,n}$ with $\mathfrak{T}_{m,n} = \langle g_2 \rangle$. In view of Corollary 2.5, there are integers $\alpha_2, \beta_2 \in \mathbb{N}_0$ such that $o(g_2) = |\mathfrak{T}_{m,n}| = 2^{\alpha_2} \times 3^{\beta_2}$. Since

$$o(g_2^{2^{\alpha_2}}) = 3^{\beta_2} \text{ and } o(g_2^{3^{\beta_2}}) = 2^{\alpha_2},$$

by Lemma 2.12 and Lemma 2.13 we can deduce that $\alpha_2 \leq 2$, $\beta_2 \leq 1$ and so $|\mathfrak{T}_{m,n}|$ divides 12. Since the element $t = (-1,0) \in \mathfrak{T}_{m,n}$ is of order 2, it follows that 2 divides $|\mathfrak{T}_{m,n}|$. Therefore, $|\mathfrak{T}_{m,n}| \in \{2,4,6,12\}$. We claim that $|\mathfrak{T}_{m,n}| \neq 12$. Assume the opposite. Then, there exists an element $h \in \mathfrak{T}_{m,n}$ such that $\mathfrak{T}_{m,n} = \langle h \rangle$ and $o(h) = 12$. Let $h_1 = (a,b) \in \langle h \rangle$ be an element of order 12. Then, by Lemma 2.11 we see that b divides 3. Hence, $b \in \{\pm 1, \pm 3\}$. Since $o(h) = 12$, one sees that there are exactly 4 distinct elements of order 12 in the group $\langle h \rangle = \mathfrak{T}_{m,n}$. Thus, by Lemma 2.10 for each $b \in \{\pm 1, \pm 3\}$ there is a unique integer a such that $h_1 = (a,b) \in \langle h \rangle$ and $o(h_1) = 12$. Let $h_2 = (c,d)$ be an element of $\langle h \rangle$ with $o(h_2) = 6$. Then, by Lemma 2.11 we see that d divides 3. Hence, $d \in \{\pm 1, \pm 3\}$. So, there is a unique integer a such that $h_3 = (a,d) \in \langle h \rangle$ and $o(h_3) = 12$. From the relations $a^2 + mad + nd^2 = 1$ and $c^2 + mcd + nd^2 = 1$, we get $(a-c)(a+c+md) = 0$. Since $o(h_2) = 6$ and $o(h_3) = 12$, it follows that $h_2 \neq h_3$ and so $a \neq c$. Thus, from the relations $a - c \neq 0$ and $(a-c)(a+c+md) = 0$, it is concluded that $a + c + md = 0$. Therefore, $h_3^{-1} = (a+md, -d) = (-c, -d) = (-1,0) * h_2$, which implies that $(h_3^{-1})^6 = (-1,0)^6 * h_2^6 = e$. Hence, $12 = o(h_3) = o(h_3^{-1}) \leq 6$, which is a contradiction. Therefore, $\mathfrak{T}_{m,n}$ is a finite cyclic group with $|\mathfrak{T}_{m,n}| \in \{2,4,6\}$. Consequently, $\mathfrak{T}_{m,n}$ is isomorphic to $\mathbb{Z}_k$ for some $k \in \{2,4,6\}$, as required. □

The following auxiliary lemmas are needed in the proof of Theorem 2.20.

Lemma 2.11. *Let m and n be two integers and set $\delta := m^2 - 4n$. If $\delta < 0$, then the Abelian group $\mathfrak{B}_{m,n}$ is isomorphic to $\mathbb{Z}_k$ for some $k \in \{2, 4, 6\}$.*

Proof. By Theorem 2.14 it is enough to prove that $\mathfrak{B}_{m,n} = \mathfrak{T}_{m,n}$. Also, in order to prove this assertion, it suffices for us to prove that $\mathfrak{B}_{m,n}$ is a finite group. Assume that $(a, b) \in \mathfrak{B}_{m,n}$. Then, by the definition we have $a^2 + mab + nb^2 = 1$. Therefore, $(2a + mb)^2 - \delta b^2 = 4(a^2 + mab + nb^2) = 4$. Hence,

$$0 \leq (2a+mb)^2 \leq (2a+mb)^2 - \delta b^2 = 4, \text{ and } 0 \leq b^2 \leq -\delta b^2 \leq (2a+mb)^2 - \delta b^2 = 4.$$

Therefore, $\{2a + mb, b\} \subseteq \{0, \pm 1, \pm 2\}$. Thus, $\mathfrak{B}_{m,n}$ is a finite group, as required. □

Lemma 2.12. *Let m and n be two integers and set $\delta := m^2 - 4n$. If $\delta = 0$, then the Abelian group $\mathfrak{B}_{m,n}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.*

Proof. Assume that $(a, b) \in \mathfrak{B}_{m,n}$. Then, by the definition we have $a^2 + mab + nb^2 = 1$. Therefore, $(2a + mb)^2 = (2a + mb)^2 - \delta b^2 = 4(a^2 + mab + nb^2) = 4$. Hence, $2a + mb = \pm 2$ and so (a, b) is a solution to one of the two-variable linear Diophantine equations $2x + my = 2$ or $2x + my = -2$. By solving these linear Diophantine equations we obtain, $(a, b) = (\pm 1 + \frac{mk}{\mu}, \frac{-2k}{\mu}) \in \mathfrak{B}_{m,n}$, where $k \in \mathbb{Z}$ and μ is the greatest common divisor of the integers 2 and m.

Set $t := (-1, 0)$ and $g := (1 + \frac{m}{\mu}, \frac{-2}{\mu})$. Then, by using induction on k and applying the relation $m^2 - 4n = 0$, it can be seen that

$$g^k = (1 + \frac{mk}{\mu}, \frac{-2k}{\mu}), \text{ and } g^{-k} = (1 - \frac{mk}{\mu}, \frac{2k}{\mu}),$$

for each $k \in \mathbb{N}$. Therefore, $g^k = (1 + \frac{mk}{\mu}, \frac{-2k}{\mu})$ and $t * g^{-k} = (-1 + \frac{mk}{\mu}, \frac{-2k}{\mu})$, for each $k \in \mathbb{Z}$. Hence,

$$\mathfrak{B}_{m,n} = \left\{(\pm 1 + \frac{mk}{\mu}, \frac{-2k}{\mu}) \ : \ k \in \mathbb{Z}\right\} = \left\{t^\ell * g^k \ : \ \ell, k \in \mathbb{Z}\right\} = \langle t \rangle * \langle g \rangle.$$

Furthermore, from the relations $o(g) = \infty$ and $o(t) = 2$, we can deduce that $\langle t \rangle \cap \langle g \rangle = \{e\}$. Therefore, $\mathfrak{B}_{m,n} = \langle t \rangle \oplus \langle g \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}$, as required. □

Lemma 2.13. *Let m and n be two integers and set $\delta := m^2 - 4n$. If δ is a positive perfect square integer, then the Abelian group $\mathfrak{B}_{m,n}$ is isomorphic to $\mathbb{Z}_2$.*

Proof. By assumption there is a positive integer λ such that $m^2 - 4n = \delta = \lambda^2$. Suppose that $(a, b) \in \mathfrak{B}_{m,n}$. Then, by the definition we have $a^2 + mab + nb^2 = 1$. Therefore,

$$(2a + mb + \lambda b)(2a + mb - \lambda b) = (2a + mb)^2 - \delta b^2 = 4(a^2 + mab + nb^2) = 4.$$

In fact, there are precisely six cases. In the following four cases:
Case 1. $2a + mb + \lambda b = 1$ and $2a + mb - \lambda b = 4$.

Case 2. $2a+mb+\lambda b=4$ and $2a+mb-\lambda b=1$.
Case 3. $2a+mb+\lambda b=-1$ and $2a+mb-\lambda b=-4$.
Case 4. $2a+mb+\lambda b=-4$ and $2a+mb-\lambda b=-1$, we see that $2a+mb=\pm\frac{5}{2}$, contradicting the fact that $2a+mb$ is an integer. Also, in the following two remainder cases,
Case 5. $2a+mb+\lambda b=2$ and $2a+mb-\lambda b=2$, Case 6. $2a+mb+\lambda b=-2$ and $2a+mb-\lambda b=-2$, we see that $(a,b)=(\pm 1,0)$. Therefore, $\mathfrak{B}_{m,n}=\{(1,0),(-1,0)\}\simeq\mathbb{Z}_2$, as required. □

Recall that *Pell's equation*, also called the *Pell-Fermat equation*, is any Diophantine equation of the form $x^2-ny^2=1$, where n is a given positive nonsquare integer. It is well-known that *Pell's equation* has a infinite solutions. Also, this equation has a solution (a_1,b_1) with $a_1\geq 1$ and $b_1\geq 1$ which has some special properties and is called *the fundamental solution.* Furthermore, once the fundamental solution is found, all remaining solutions may be calculated algebraically from

$$a_k+b_k\sqrt{n}=(a_1+b_1\sqrt{n})^k,$$

expanding the right side, equating coefficients of $\sqrt{n}$ on both sides, and equating the other terms on both sides. This yields the recurrence relation

$$(a_{k+1},b_{k+1})=(a_1a_k+nb_1b_k,a_1b_k+b_1a_k).$$

In this situation, the set of all solutions of the equation $x^2-ny^2=1$ is equal to

$$\{(\pm 1,0)\}\cup\{(\pm a_k,\pm b_k)\ :\ k\in\mathbb{N}\}.$$

For more details see [1]. In order to establish our next lemma, we use a proof similar to the proof of [1, p. 180, Theorem 7].

Lemma 2.14. *Let m and n be two integers and set $\delta:=m^2-4n$. If δ is a positive nonsquare integer, then the Abelian group $\mathfrak{B}_{m,n}$ is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}$.*

Proof. Let (u_1,v_1) denote the fundamental solution of the *Pell's equation* $x^2-\delta y^2=1$. Set $(\alpha,\beta):=(u_1-mv_1,2v_1)$. Then, it is easy to see that $(\alpha,\beta)\in\mathfrak{B}_{m,n}$, $\alpha+\frac{m\beta}{2}=u_1>0$ and $\frac{\beta}{2}=v_1>0$. Set $M:=\alpha+\frac{m\beta}{2}+\frac{\beta}{2}\sqrt{\delta}$. If $(\alpha',\beta')\in\mathfrak{B}_{m,n}$ is an element such that $\alpha'+\frac{m\beta'}{2}>0$ and $\frac{\beta'}{2}>0$, then the condition

$$\alpha'+\frac{m\beta'}{2}+\frac{\beta'}{2}\sqrt{\delta}\leq M,$$

implies that $\alpha'+\frac{m\beta'}{2}\leq M$ and $\frac{\beta'}{2}\leq M$. Therefore, $1\leq\beta'\leq 2M$ and $-|m|M\leq\alpha'\leq(1+|m|)M$. Thus, in particular, there are only finitely many choices for the integers α' and β'. Let us choose $g=(a_1,b_1)\in\mathfrak{B}_{m,n}$ for which $a_1+\frac{mb_1}{2}>0$, $\frac{b_1}{2}>0$ and $a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}$ is least. This is possible since there are only finitely many elements $(\alpha',\beta')\in\mathfrak{B}_{m,n}$ such that $\alpha'+\frac{m\beta'}{2}>0$ and $\frac{\beta'}{2}>0$, and

$$\alpha'+\frac{m\beta'}{2}+\frac{\beta'}{2}\sqrt{\delta}\leq M.$$

For each positive integer k, define a_k and b_k by

$$a_k + \frac{mb_k}{2} + \frac{b_k}{2}\sqrt{\delta} = \left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)^k . \tag{2.1}$$

Indeed, since by the hypothesis δ is a positive nonsquare integer, we see that $\sqrt{\delta}$ is an irrational number. Therefore, for each positive integer k, the elements a_k and b_k can be calculated algebraically from (2.18.1), expanding the right side, equating coefficients of $\sqrt{\delta}$ on both sides, and equating the other terms on both sides.

By using induction on k, we prove that $a_k + \frac{mb_k}{2} > 0$, $\frac{b_k}{2} > 0$ and $(a_k, b_k) = g^k \in \mathfrak{B}_{m,n}$, for each $k \in \mathbb{N}$. For $k = 1$ the assertion holds by the hypothesis. Now, let $k > 1$ and assume that the result has been proved for $k - 1$. Then, by inductive assumption we know that $a_{k-1} + \frac{mb_{k-1}}{2} > 0$, $\frac{b_{k-1}}{2} > 0$ and $(a_{k-1}, b_{k-1}) = g^{k-1} \in \mathfrak{B}_{m,n}$. By using the fact that $\sqrt{\delta}$ is an irrational number, from the relations

$$\begin{aligned} a_k + \frac{mb_k}{2} + \frac{b_k}{2}\sqrt{\delta} &= \left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)^k \\ &= \left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)^{k-1} \\ &= \left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)\left(a_{k-1} + \frac{mb_{k-1}}{2} + \frac{b_{k-1}}{2}\sqrt{\delta}\right), \end{aligned}$$

we obtain, $b_k = a_1 b_{k-1} + b_1 a_{k-1} + m b_1 b_{k-1}$ and

$$\begin{aligned} a_k + \frac{mb_k}{2} &= a_1 a_{k-1} + \frac{m(a_1 b_{k-1} + b_1 a_{k-1})}{2} + \frac{m^2 b_1 b_{k-1}}{4} + \frac{\delta b_1 b_{k-1}}{4} \\ &= a_1 a_{k-1} + \frac{m(a_1 b_{k-1} + b_1 a_{k-1})}{2} + \frac{m^2 b_1 b_{k-1}}{4} + \frac{(m^2 - 4n) b_1 b_{k-1}}{4} \\ &= a_1 a_{k-1} - n b_1 b_{k-1} + \frac{m(a_1 b_{k-1} + b_1 a_{k-1} + m b_1 b_{k-1})}{2} \\ &= a_1 a_{k-1} - n b_1 b_{k-1} + \frac{mb_k}{2}, \end{aligned}$$

which implies that $a_k = a_1 a_{k-1} - n b_1 b_{k-1}$. Thus,

$$(a_k, b_k) = (a_1 a_{k-1} - n b_1 b_{k-1}, a_1 b_{k-1} + b_1 a_{k-1} + m b_1 b_{k-1}) = g * g^{k-1} = g^k.$$

Also, the relations

$$\frac{b_k}{2} = \left(a_1 + \frac{mb_1}{2}\right)\left(\frac{b_{k-1}}{2}\right) + \left(a_{k-1} + \frac{mb_{k-1}}{2}\right)\left(\frac{b_1}{2}\right),$$

and

$$a_k + \frac{mb_k}{2} = \left(a_1 + \frac{mb_1}{2}\right)\left(a_{k-1} + \frac{mb_{k-1}}{2}\right) + \delta\left(\frac{b_1}{2}\right)\left(\frac{b_{k-1}}{2}\right),$$

together with the hypothesis $a_1+\frac{mb_1}{2}>0$, $a_{k-1}+\frac{mb_{k-1}}{2}>0$, $\frac{b_1}{2}>0$, $\frac{b_{k-1}}{2}>0$, and $\delta>0$, imply that $a_k+\frac{mb_k}{2}>0$ and $\frac{b_k}{2}>0$. This completes the inductive step.

We claim that $o(g)=\infty$. Assume the opposite and let $o(g)=j<\infty$. Then, we see that $g^j=(a_j,b_j)=(1,0)$. Therefore, $b_j=0$, which is impossible since $\frac{b_j}{2}>0$. Thus, $o(g)=\infty$ and so the cyclic subgroup $\langle g\rangle$ of $\mathfrak{B}_{m,n}$ is isomorphic to $\mathbb{Z}$.

Let $h=(a',b')\in(\mathfrak{B}_{m,n}\setminus\mathfrak{T}_{m,n})$. Then, by the definition we have $o(h)=\infty$. Set $t=(-1,0)\in\mathfrak{B}_{m,n}$. Since $o(t)=2$, it is clear that $t\in\mathfrak{T}_{m,n}$. Also, from the assumption $o(h)=\infty$ it follows that $b'\neq 0$ and the elements $h,h^{-1},t*h,t*h^{-1}$ are different. Therefore, the relation

$$\left\{h,h^{-1},t*h,t*h^{-1}\right\}=\left\{(a',b'),(a'+mb',-b'),(-a',-b'),(-a'-mb',b')\right\},$$

implies that $2a'+mb'\neq 0$ and hence $a'+\frac{mb'}{2}\neq 0$. Since

$$\left\{(u+\frac{mv}{2},\frac{v}{2})\ :\ (u,v)\in\left\{h,h^{-1},t*h,t*h^{-1}\right\}\right\}=\left\{(\pm(a'+\frac{mb'}{2}),\pm\frac{b'}{2})\right\},$$

we can find an element $(a,b)\in\{h,h^{-1},t*h,t*h^{-1}\}$ such that $a+\frac{mb}{2}>0$ and $\frac{b}{2}>0$. We show that $(a,b)=g^\ell$ for some $\ell\in\mathbb{N}$.

Since (a_1,b_1) was chosen as the element of $\mathfrak{B}_{m,n}$ for which $a_1+\frac{mb_1}{2}>0$, $\frac{b_1}{2}>0$ and $a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}$ is least, we see that

$$a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\leq a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}. \tag{2.2}$$

We assert that there is a positive integer ℓ such that

$$\left(a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\right)^\ell\leq a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}<\left(a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\right)^{\ell+1}. \tag{2.3}$$

Since by the hypothesis δ is a positive nonsquare integer, it follows that $\delta\geq 2$. Therefore, by using the hypothesis $a_1+\frac{mb_1}{2}>0$ and $\frac{b_1}{2}>0$, one sees that

$$a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}=\frac{2a_1+mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\geq\frac{1}{2}+\frac{1}{2}\sqrt{\delta}\geq\frac{1}{2}+\frac{1}{2}\sqrt{2}>\frac{1}{2}+\frac{1}{2}=1.$$

Thus, $a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}>1$ and hence the powers of $a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}$, became arbitrary large. So, there is a largest value of ℓ for which

$$\left(a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\right)^\ell\leq a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}.$$

Furthermore, by the relation (2.18.2) we know that this largest value of ℓ is at least 1. Moreover, it is clear that this largest value of ℓ forces (2.18.3) to hold. Let us multiply (2.18.3) by $(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta})^\ell$, which is positive since $a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta} > 0$ and

$$\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right) = a_1^2 + ma_1b_1 + nb_1^2 = 1.$$

Then, we see that

$$1 \leq \left(a + \frac{mb}{2} + \frac{b}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)^\ell < a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}. \tag{2.4}$$

Since $g = (a_1, b_1)$, $g^\ell = (a_\ell, b_\ell) \in \mathfrak{B}_{m,n}$, one sees that

$$\begin{aligned}&\left(a_\ell + \frac{mb_\ell}{2} + \frac{b_\ell}{2}\sqrt{\delta}\right)\left(a_\ell + \frac{mb_\ell}{2} - \frac{b_\ell}{2}\sqrt{\delta}\right)\\ &= \left(a_\ell + \frac{mb_\ell}{2}\right)^2 - \delta\left(\frac{b_\ell}{2}\right)^2 = a_\ell^2 + ma_\ell b_\ell + nb_\ell^2 = 1,\end{aligned}$$

and

$$\begin{aligned}&\left(a_\ell + \frac{mb_\ell}{2} + \frac{b_\ell}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)^\ell\\ &= \left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)^\ell\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)^\ell\\ &= \left(\left(a_1 + \frac{mb_1}{2} + \frac{b_1}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)\right)^\ell\\ &= \left(\left(a_1 + \frac{mb_1}{2}\right)^2 - \delta\left(\frac{b_1}{2}\right)^2\right)^\ell\\ &= \left(a_1^2 + ma_1b_1 + nb_1^2\right)^\ell = 1^\ell = 1.\end{aligned}$$

Therefore,

$$\begin{aligned}&\left(a_\ell + \frac{mb_\ell}{2} + \frac{b_\ell}{2}\sqrt{\delta}\right)\left(a_\ell + \frac{mb_\ell}{2} - \frac{b_\ell}{2}\sqrt{\delta}\right) = 1\\ &= \left(a_\ell + \frac{mb_\ell}{2} + \frac{b_\ell}{2}\sqrt{\delta}\right)\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)^\ell,\end{aligned}$$

and so

$$\left(a_1 + \frac{mb_1}{2} - \frac{b_1}{2}\sqrt{\delta}\right)^\ell = a_\ell + \frac{mb_\ell}{2} - \frac{b_\ell}{2}\sqrt{\delta}.$$

Set $c := aa_\ell + mab_\ell + nbb_\ell$, and $d := ba_\ell - ab_\ell$. Obviously, $c, d \in \mathbb{Z}$. Also, it is straightforward to see that

$$c + \frac{md}{2} = \left(a + \frac{mb}{2}\right)\left(a_\ell + \frac{mb_\ell}{2}\right) - \delta\left(\frac{b}{2}\right)\left(\frac{b_\ell}{2}\right)$$

and

$$\frac{d}{2}=\left(\frac{b}{2}\right)\left(a_\ell+\frac{mb_\ell}{2}\right)-\left(a+\frac{mb}{2}\right)\left(\frac{b_\ell}{2}\right).$$

So, we have

$$\begin{aligned}&\left(a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}\right)\left(a_1+\frac{mb_1}{2}-\frac{b_1}{2}\sqrt{\delta}\right)^\ell\\ &=\left(a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}\right)\left(a_\ell+\frac{mb_\ell}{2}-\frac{b_\ell}{2}\sqrt{\delta}\right)=c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}.\end{aligned}$$

Moreover, it is easy to see that

$$\left(a+\frac{mb}{2}-\frac{b}{2}\sqrt{\delta}\right)\left(a_\ell+\frac{mb_\ell}{2}+\frac{b_\ell}{2}\sqrt{\delta}\right)=c+\frac{md}{2}-\frac{d}{2}\sqrt{\delta}.$$

By using these relations it can be seen that

$$\begin{aligned}c^2+mcd+nd^2 &= \left(c+\frac{md}{2}\right)^2-\delta\left(\frac{d}{2}\right)^2\\ &= \left(\left(a+\frac{mb}{2}\right)^2-\delta\left(\frac{b}{2}\right)^2\right)\left(\left(a_\ell+\frac{mb_\ell}{2}\right)^2-\delta\left(\frac{b_\ell}{2}\right)^2\right)\\ &= \left(a^2+mab+nb^2\right)\left(a_\ell^2+ma_\ell b_\ell+nb_\ell^2\right)\\ &= (1)(1)=1.\end{aligned}$$

Therefore, $(c,d)\in\mathfrak{B}_{m,n}$. Furthermore, (2.18.4) asserts that

$$1\leq c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}<a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}. \tag{2.5}$$

We claim that $(c,d)=(1,0)$. Assume the opposite. If $d=0$, then from the relation $c^2+mcd+nd^2=1$ we get $c=\pm1$ and so, by (2.18.5) it follows that $c=1$. Thus, $(c,d)=(1,0)$ which is a contradiction. Also, if $c+\frac{md}{2}=0$, then from the relation

$$\left(c+\frac{md}{2}\right)^2-\delta\left(\frac{d}{2}\right)^2=1,$$

we can deduce $-\delta\left(\frac{d}{2}\right)^2=1$ and so $\delta<0$, which is a contradiction. Hence, $d\neq0$ and $c+\frac{md}{2}\neq0$. In this situation we claim that $c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}\leq1$. Assume the opposite. Then, we have $c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}>1$. Let us consider the following three cases:

Case 1. $c+\frac{md}{2}<0$ and $\frac{d}{2}<0$. Then, $c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}<0$, which contradicts the assumption that $c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}>1$.

Case 2. $c+\frac{md}{2}<0$ and $\frac{d}{2}>0$. Then

$$-\left(c+\frac{md}{2}\right)+\frac{d}{2}\sqrt{\delta}>c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}>1,$$

and so

$$\begin{aligned} -1 &= -(c^2+mcd+nd^2) = \delta\left(\frac{d}{2}\right)^2 - \left(c+\frac{md}{2}\right)^2 \\ &= \left(-\left(c+\frac{md}{2}\right)+\frac{d}{2}\sqrt{\delta}\right)\left(c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}\right) > 1, \end{aligned}$$

which is absurd.
Case 3. $c+\frac{md}{2}>0$ and $\frac{d}{2}<0$. Then

$$c+\frac{md}{2}-\frac{d}{2}\sqrt{\delta} > c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta} > 1,$$

and so

$$\begin{aligned} 1 = c^2+mcd+nd^2 &= \left(c+\frac{md}{2}\right)^2 - \delta\left(\frac{d}{2}\right)^2 \\ &= \left(c+\frac{md}{2}-\frac{d}{2}\sqrt{\delta}\right)\left(c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}\right) > 1, \end{aligned}$$

which is also absurd. Thus, the only possible case is $c+\frac{md}{2}>0$ and $\frac{d}{2}>0$. However, if this is the case, then (2.18.5) contradicts the way in which (a_1,b_1) was chosen. Therefore, we must have

$$c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta} \leq 1.$$

Then, (2.18.5) implies that

$$c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta} = 1.$$

So, by using the fact that $\sqrt{\delta}$ is an irrational number, we can deduce that $(c,d)=(1,0)$, which is a contradiction. Thus, we have $(c,d)=(1,0)$ and hence $c+\frac{md}{2}+\frac{d}{2}\sqrt{\delta}=1$. Therefore,

$$\left(a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta}\right)\left(a_1+\frac{mb_1}{2}-\frac{b_1}{2}\sqrt{\delta}\right)^{\ell} = 1.$$

Multiplying both sides of this equation by $\left(a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\right)^{\ell}$, we see that

$$a+\frac{mb}{2}+\frac{b}{2}\sqrt{\delta} = \left(a_1+\frac{mb_1}{2}+\frac{b_1}{2}\sqrt{\delta}\right)^{\ell} = a_\ell+\frac{mb_\ell}{2}+\frac{b_\ell}{2}\sqrt{\delta}.$$

Thus, by using the fact that $\sqrt{\delta}$ is an irrational number, we get $(a,b)=(a_\ell,b_\ell)=g^\ell$. Therefore, $g^\ell=(a,b)\in\{h,h^{-1},t{*}h,t{*}h^{-1}\}$ and so $h=t^rg^s$ for some integers r and s. Since $t\in\mathfrak{T}_{m,n}$, we see that $h\in\mathfrak{T}_{m,n}*\langle g\rangle$. So,

$$(\mathfrak{B}_{m,n}\setminus\mathfrak{T}_{m,n})\subseteq\mathfrak{T}_{m,n}*\langle g\rangle.$$

Hence,

$$\mathfrak{B}_{m,n} = (\mathfrak{B}_{m,n} \setminus \mathfrak{T}_{m,n}) \cup \mathfrak{T}_{m,n} \subseteq \mathfrak{T}_{m,n} * \langle g \rangle \subseteq \mathfrak{B}_{m,n},$$

which means that $\mathfrak{B}_{m,n} = \mathfrak{T}_{m,n} * \langle g \rangle$. Also, by using the assumption $o(g) = \infty$, we can deduce that $\mathfrak{T}_{m,n} \cap \langle g \rangle = \{e\}$. Therefore, $\mathfrak{B}_{m,n} = \mathfrak{T}_{m,n} \oplus \langle g \rangle$. By Theorem 2.14 there exists an element $\theta \in \mathfrak{T}_{m,n}$ such that $\mathfrak{T}_{m,n} = \langle \theta \rangle$. Set $h' := \theta * g$. Since $h' \in (\mathfrak{B}_{m,n} \setminus \mathfrak{T}_{m,n})$, by the same argument we can find integers $r', s' \in \mathbb{Z}$ such that $\theta * g = h' = t^{r'} * g^{s'}$. Since $\mathfrak{B}_{m,n} = \mathfrak{T}_{m,n} \oplus \langle g \rangle$ and $\theta, t \in \mathfrak{T}_{m,n}$ it is concluded that $\theta = t^{r'} \in \langle t \rangle$. Therefore, $\mathfrak{T}_{m,n} = \langle \theta \rangle \subseteq \langle t \rangle \subseteq \mathfrak{T}_{m,n}$, which means that $\mathfrak{T}_{m,n} = \langle t \rangle = \{e, t\}$. Thus, $\mathfrak{B}_{m,n} = \mathfrak{T}_{m,n} \oplus \langle g \rangle = \langle t \rangle \oplus \langle g \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}$. □

Corollary 2.3. *Assume that n is a given positive nonsquare integer. Then, the Abelian group of all integer solutions of the Pell's equatuion $x^2 - ny^2 = 1$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.*

Proof. The assertion follows from Lemma 2.18. □

We are now in a position to use the previous results to produce a proof of our main theorem.

Theorem 2.3. *Let m and n be two integers. Then, the Abelian group $\mathfrak{B}_{m,n}$ is isomorphic to one of the groups $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}$.*

Proof. The assertion follows from Lemmas 2.15, 2.16, 2.17 and 2.18. □

Example 2.4. (i) Assume that $n > 0$ is a given perfect square integer. Then, by Lemma 2.17 we see that $\mathfrak{B}_{0,-n} = \mathfrak{T}_{0,-n} = \{(1,0), (-1,0)\} \simeq \mathbb{Z}_2$.

(ii) Assume that n is a given positive nonsquare integer. Then, by Corollary 2.19 we have $\mathfrak{B}_{0,-n} \simeq \mathbb{Z}_2 \times \mathbb{Z}$ and so $\mathfrak{T}_{0,-n} = \{(1,0), (-1,0)\} \simeq \mathbb{Z}_2$.

(iii) Let $g = (0,1) \in \mathfrak{B}_{0,1} = \{(1,0), (-1,0), (0,1), (0,-1)\}$. Then, one can see that $o(g) = 4$ and $\mathfrak{B}_{0,1} = \mathfrak{T}_{0,1} = \langle g \rangle \simeq \mathbb{Z}_4$.

(iv) Let $g = (0,-1) \in \mathfrak{B}_{-1,1}$. Then, it is easy to see that $o(g) = 6$ and so, by Theorem 2.14 and Lemma 2.15 we can deduce that $\mathfrak{B}_{-1,1} = \mathfrak{T}_{-1,1} = \langle g \rangle \simeq \mathbb{Z}_6$.

Remark 2.5. Let $(R, +, \cdot)$ be a commutative ring with the identity element and η, ξ, ζ be three arbitrary elements of R. Set

$$S(R, \eta, \xi, \zeta) := \{(u,v) \in R \times R \ : \ u^2 + \eta uv + \xi v^2 = \zeta\}.$$

Assume that $S(R, \eta, \xi, \zeta) \neq \emptyset$ and $(u,v) \in S(R, \eta, \xi, \zeta)$. Then, for each $(a,b) \in G(R, \eta, \xi)$ the element

$$(a,b) \cdot (u,v) := (au - \xi bv, bu + av + \eta bv),$$

belongs to $S(R, \eta, \xi, \zeta)$. In fact, by this definition the group $G(R, \eta, \xi)$ acts on the set $S(R, \eta, \xi, \zeta)$, provided that $S(R, \eta, \xi, \zeta) \neq \emptyset$.

References

[1] W. W. Adams and L. J. Goldstein, *Introduction to number theory*, Prentice-Hall, Inc, 1976.

[2] M. Hall, *The theory of groups*, New York: The Macmillan Company, 1959.

[3] J. McKay, *Another proof of Cauchy's group theorem*, American Math. Monthly, 66 (1959), 119.

Accepted: November 21, 2022