ALGEBRAIC AND GEOMETRIC PROPERTIES OF LATTICE WALKS WITH STEPS OF EQUAL LENGTH

KRZYSZTOF KOŁODZIEJCZYK✉ and RAFAŁ SAŁAPATA

In memory of Professor Czesław Ryll-Nardzewski whose question is answered in this note.

Abstract

A lattice walk with all steps having the same length d is called a d-walk. Denote by $\mathcal{T}_d$ the terminal set, that is, the set of all lattice points that can be reached from the origin by means of a d-walk. We examine some geometric and algebraic properties of the terminal set. After observing that $(\mathcal{T}_d, +)$ is a normal subgroup of the group $(\mathbb{Z}^N, +)$, we ask questions about the quotient group $\mathbb{Z}^N/\mathcal{T}_d$ and give the number of elements of $\mathbb{Z}^2/\mathcal{T}_d$ in terms of d. To establish this result, we use several consequences of Fermat's theorem about representations of prime numbers of the form $4k + 1$ as the sum of two squares. One of the consequences is the fact, observed by Sierpiński, that every natural power of such a prime number has exactly one relatively prime representation. We provide explicit formulas for the relatively prime integers in this representation.

1. Introduction

A *lattice point* in $\mathbb{R}^N$ is a point with integer coordinates. The set of all lattice points in $\mathbb{R}^N$ is denoted by $\mathbb{Z}^N$. By a *lattice walk* or *lattice path* in $\mathbb{R}^N$ we mean an ordered sequence of lattice points $\mathcal{W} = (w_0, w_1, \ldots, w_m)$. The point w_0 is called the *initial point* and w_m is called the *terminal point* of $\mathcal{W}$. Without loss of generality, we can assume that $w_0 = 0$. With this assumption, there is a one-to-one correspondence between a lattice walk $\mathcal{W}$ and the ordered sequence $\mathcal{U} = (u_1, \ldots, u_m)$ of vectors, called *steps*, where $u_i = w_i - w_{i-1}$ for $i = 1, \ldots, m$. Thus, we shall alternatively use $\mathcal{W}$ or $\mathcal{U}$ to represent the same lattice walk.

There are many aspects of research dealing with lattice points and, in particular, with lattice paths. We refer the reader to [1, 3, 6, 7, 10, 11], where various problems for different types of lattice walks are considered.

338

To present the purpose of this note, we need several definitions. A lattice walk $\mathcal{U} = (u_1, \ldots, u_m)$ is called a *d-walk* if all its steps have the same length d, that is, $\|u_i\| = d$ for $i = 1, \ldots, m$, where $\|x\|$ denotes the Euclidean norm of x.

A positive real number d is said to be *N-admissible* if there exists $v \in \mathbb{Z}^N$ such that $\|v\| = d$ or, in other words, if

$$U_d = \{v \in \mathbb{Z}^N : \|v\| = d\} \neq \emptyset.$$

Obviously, d is N-admissible if and only if d^2 has a representation as a sum of N squares.

For $x = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, by $\gcd(x)$ we denote the number $\gcd(x_1, \ldots, x_N)$. If there exists a point $x \in U_d$ with $\gcd(x) = 1$, then we say that d^2 has a *relatively prime* representation as a sum of N squares. In such a case, the real number d is called *N-reduced*. A very important class of N-reduced lattice walks are 1-walks using steps $u_i \in \{\pm e_1, \ldots, \pm e_N\}$, where $e_1, \ldots, e_N$ denote the standard unit vectors in $\mathbb{R}^N$.

For an N-admissible real number d, we define the *terminal set* $\mathcal{T}_d$ as

$$\mathcal{T}_d = \{x \in \mathbb{Z}^N : x \text{ is the terminal point in a } d\text{-walk from the origin}\}.$$

It is obvious, for 1-walks in $\mathbb{R}^N$ using steps $u_i \in \{\pm e_1, \ldots, \pm e_N\}$, that $\mathcal{T}_d = \mathbb{R}^N$.

In [7] we proved that $\mathcal{T}_d = \mathbb{R}^2$ if and only if d is a 2-reduced real number whose square, d^2, is odd. In this note, we explore the terminal set $\mathcal{T}_d$ further and study its geometric and algebraic properties. In Section 4, we show that $(\mathcal{T}_d, +)$ is a normal subgroup of $(\mathbb{Z}^N, +)$ and that $\mathcal{T}_d$ is a sublattice of $\mathbb{Z}^N$. Therefore questions about the quotient $\mathbb{Z}^N / \mathcal{T}_d$ are well motivated. The main result of this note is in Section 5 where we provide a detailed analysis of the number of elements of $\mathbb{Z}^2 / \mathcal{T}_d$ in relation to number theoretical properties of d. This is done by using some consequences of Fermat's theorem about representations of prime numbers of the form $4k + 1$ as sums of two squares. One of the consequences is the known fact, observed by Sierpiński [8], that every power (with a natural exponent) of such a prime number has a unique relatively prime representation. In Section 2, we provide explicit formulas for the relatively prime integers appearing in this representation. If L is a sublattice of $\mathbb{Z}^N$, the problem of counting the number of elements in the quotient group $\mathbb{Z}^N / L$ is of great interest. In [4, Theorem 2.3.19], this question is answered several times in relation to bases of the sublattice L. However, in the special case when $L = \mathcal{T}_d$, it would be nice to have the number of elements of $\mathbb{Z}^N / \mathcal{T}_d$ given in relation to d. This is why we end our note with a problem to express the cardinality of $\mathbb{Z}^N / \mathcal{T}_d$ in terms of d and (possibly) of N.

2. 2-reduced numbers

To speak about d-walks, we need d to be 2-admissible. From results in elementary number theory, a real number d is 2-admissible if and only if d^2 has the form

$$d^2 = 2^{2\beta + \alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r} (q_1^{\beta_1} \cdots q_s^{\beta_s})^2, \tag{2.1}$$

where p_i and q_j are distinct prime numbers such that $p_i \equiv 1 \pmod 4$ for $i = 1, \ldots, r$, $q_j \equiv 3 \pmod 4$ for $j = 1, \ldots, s$, $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \mathbb{N}, \beta, r, s \in \mathbb{N} \cup \{0\}$ and $\alpha \in \{0, 1\}$.

In particular, we will deal with 2-reduced numbers. This is why we will need some consequences of Fermat's theorem about representations of natural numbers as sums of squares. A rephrased version of Fermat's theorem reads as follows.

THEOREM 2.1 (Fermat). *Let p be a prime number of the form $p \equiv 1 \pmod 4$. Then $d = \sqrt{p}$ is 2-reduced.*

Sierpiński [8, 9] proved that every power (with a natural exponent) of a prime of the form $4k + 1$ has unique relatively prime representation as the sum of two squares. Below we provide explicit formulas for the integers appearing in this unique representation.

THEOREM 2.2. *Let p be a prime number of the form $p \equiv 1 \pmod 4$ with the representation $p = a^2 + b^2$ as the sum of squares. Then, for every $\alpha \in \mathbb{N}$, the number $\sqrt{p^\alpha}$ is 2-reduced, that is, $p^\alpha = x_\alpha^2 + y_\alpha^2$ for relatively prime numbers x_α and y_α given by*

$$x_\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{2k} (-1)^k a^{2k} b^{\alpha - 2k} \quad and \quad y_\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{2k+1} (-1)^k a^{2k+1} b^{\alpha - (2k+1)}.$$

PROOF. Suppose p is a prime of the form $p \equiv 1 \pmod 4$ and $p = a^2 + b^2$. Obviously, a and b are relatively prime. Moreover, $x_1 = b$ and $y_1 = a$.

Clearly, $p = (b + ia)(b - ia)$, where $i = \sqrt{-1}$. Observe that, via the binomial theorem,

$$(b + ia)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{2k} (-1)^k a^{2k} b^{\alpha - 2k} + i \sum_{k=0}^{\infty} \binom{\alpha}{2k+1} (-1)^k a^{2k} b^{\alpha - 2k} = x_\alpha + i y_\alpha.$$

Hence

$$p^\alpha = (b + ia)^\alpha (b - ia)^\alpha = (x_\alpha + iy_\alpha)(x_\alpha - iy_\alpha) = x_\alpha^2 + y_\alpha^2.$$

If x_α and y_α have a common factor greater than one, then they must both be divisible by p and so p divides $(b + ia)^\alpha$. That is, $(b + ia)(b - ia)$ divides $(b + ia)^\alpha$ and so $(b - ia)$ divides $(b + ia)^{\alpha - 1}$. This is impossible since $(b + ia)$ and $(b - ia)$ are distinct Gaussian primes. Thus x_α and y_α are relatively prime. The proof is finished. $\square$

It was pointed out to us by the editor that the formulas for x_α and y_α have already been observed by Plana (compare with [5, page 241]). We show, in addition, that the representation is relatively prime. It is worth noticing, in this context, that the following fact is true.

COROLLARY 2.3. *Let p be a prime number of the form $p \equiv 1 \pmod 4$. Then, for every $\alpha \geq 3$, the number p^α has a representation $p^\alpha = c_\alpha^2 + d_\alpha^2$ such that $p \| c_\alpha$ and $p \| d_\alpha$. Moreover, if $p = a^2 + b^2$, then*

$$c_\alpha = \sum_{k=0}^{\infty} \left[\binom{\alpha - 1}{2k} - \binom{\alpha - 1}{2k+1} \right] (-1)^k a^{2k+1} b^{\alpha - (2k+1)}$$

and

$$d_\alpha = \sum_{k=0}^{\infty} \left[\binom{\alpha-1}{2k} - \binom{\alpha-1}{2k-1} \right] (-1)^k a^{2k} b^{\alpha-2k}.$$

PROOF. Let x_α and y_α be as in Theorem 2.2. Then

$$p^\alpha = (a^2 + b^2)(x_{\alpha-1}^2 + y_{\alpha-1}^2) = (ax_{\alpha-1} - by_{\alpha-1})^2 + (bx_{\alpha-1} + ay_{\alpha-1})^2.$$

It is easy to check that

$$c_\alpha = ax_{\alpha-1} - by_{\alpha-1} \quad \text{and} \quad d_\alpha = bx_{\alpha-1} + ay_{\alpha-1}.$$

So, to complete the proof, it is enough to show that p divides c_α and d_α. For that purpose, we consider the polynomial

$$W(z) = \sum_{k=0}^{\infty} \left[\binom{\alpha-1}{2k} - \binom{\alpha-1}{2k+1} \right] (-1)^k z^{2k+1} b^{\alpha-1-2k}$$

of a complex variable z. One can easily check that, for $\alpha \geq 3$,

$$W(\pm ib) = \pm ib^\alpha \sum_{k=0}^{\infty} \left[\binom{\alpha-1}{2k} - \binom{\alpha-1}{2k+1} \right] = 0.$$

Thus $W(z) = (z^2 + b^2) \cdot W_1(z)$ for some polynomial $W_1(z)$. In particular, $W(a) = (a^2 + b^2) \cdot W_1(a)$ which means that c_α is divisible by p. In a similar way one can check that p divides d_α. The proof is finished. □

Sierpiński [8] has shown the following result.

THEOREM 2.4 (Sierpiński). *Let $t = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where p_i are distinct prime numbers of the form $p_i \equiv 1 \pmod 4$ for $i = 1, \ldots, r$ and $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$. Then t has a relatively prime representation as the sum of two squares.*

The next theorem provides a general form of 2-reduced numbers.

THEOREM 2.5. *Every real number d such that $d^2 = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where p_i are distinct prime numbers of the form $p_i \equiv 1 \pmod 4$ for $i = 1, \ldots, r$ with $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ and $\alpha \in \{0, 1\}$, is 2-reduced.*

PROOF. The case $\alpha = 0$ is considered in Theorem 2.4. If $s = 2t = 2p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then Theorem 2.4 guarantees the existence of relatively prime numbers x and y such that $t = x^2 + y^2$. Clearly,

$$s = 2(x^2 + y^2) = (x + y)^2 + (x - y)^2. \tag{2.2}$$

In view of (2.2), the numbers x and y are of different parity. Now it is easily seen that neither $x + y$ nor $x - y$ are divisible by any of the numbers $2, p_1, \ldots, p_r$. Thus $x + y$ and $x - y$ are relatively prime and d is 2-reduced. □

3. The cardinality and a property of U_d

The number of representations of a natural number n by the sum of two squares, allowing zeros and distinguishing signs and order, is usually denoted by $r_2(n)$. It is known, see [2], that

$$r_2(n) = \begin{cases} 4(\alpha_1 + 1) \cdots (\alpha_r + 1) & \text{if } n \text{ is of the form (2.1)}, \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

From (3.1), it follows that if d^2 is of the form (2.1), then

$$|U_d| = r_2(d^2) = 4(\alpha_1 + 1) \cdots (\alpha_r + 1). \tag{3.2}$$

We now introduce a notation which plays a crucial role in finding the cardinality of $\mathbb{Z}^2/\mathcal{T}_d$. Let d be a 2-admissible real number. Define

$$h_d = \min\{\gcd(v) \geq 1 : v \in U_d\}.$$

LEMMA 3.1. *Let d be a 2-admissible real number with d^2 of the form (2.1). Then*

$$h_d = 2^\beta q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

PROOF. Take a 2-admissible real number d with d^2 of the form (2.1). Denote by h the number $h = 2^\beta q_1^{\beta_1} \cdots q_s^{\beta_s}$ and consider the number $d^* = d/h$. Then

$$(d^*)^2 = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

By Theorem 2.5, there are relatively prime numbers x and y such that $(x, y) \in U_{d^*}$. Clearly, the vector (hx, hy) belongs to U_d and $\gcd(v) = h$. This means that $h_d \leq h$.

Now take any vector $v = (x, y)$ from U_d. If $h \nmid x$ or $h \nmid y$, then the vector v/h would not belong to $U_{d/h}$. This, and the obvious inclusion $hU_{d/h} \subset U_d$, would imply that $|U_{d/h}| < |U_d|$, which gives us a contradiction because, from (3.1) and (3.2), it follows that $|U_{d/h}| = |U_d|$. Thus, for every $v = (x, y) \in U_d$, $h|x$ and $h|y$ and therefore also $\gcd(v) \geq h$. This implies that $h_d \geq h$. Consequently, $h = h_d$ and the proof is finished. □

In the proof of Lemma 3.1 we have shown the following property of h_d.

REMARK 3.2. Let d be a 2-admissible real number. Then

$$h_d = \gcd\left(\bigcup_{(x,y) \in U_d} \{x, y\} \right). \tag{3.3}$$

THEOREM 3.3. *For any 2-admissible real number d,*

$$h_d \cdot U_{d/h_d} = U_d.$$

PROOF. The inclusion $h_d \cdot U_{d/h_d} \subset U_d$ is obvious. From (3.3) it follows, for every $v = (x, y) \in U_d$, that $h_d|x$ and $h_d|y$. Therefore there exists $v' = (x', y') \in U_{d/h_d}$ such that $h_d v' = v$. This means that $v \in h_d U_{d/h_d}$. Thus the inclusion $U_d \subset h_d \cdot U_{d/h_d}$ is also true and the proof is complete. □

4. The terminal set $\mathcal{T}_d$

Let d be an N-admissible real number. Recall that the terminal set $\mathcal{T}_d$ consists of all lattice points in $\mathbb{Z}^N$ that can be reached from the origin by means of a d-walk. Since d-walks use steps from the set U_d, obviously, $U_d \subset \mathcal{T}_d$. Therefore an immediate consequence of Theorem 3.3 is the following corollary.

COROLLARY 4.1. *For any 2-admissible real number d,*

$$\mathcal{T}_d = h_d \cdot \mathcal{T}_{d/h_d}.$$

It is clear that U_d is a finite set which is symmetrical with respect to the origin and all coordinate axes. The symmetry properties of U_d guarantee that the terminal set $\mathcal{T}_d$ is also symmetrical with respect to the origin and all coordinate axes. We have also the following property of U_d.

PROPOSITION 4.2. *For any permutation $\pi : \{1, \ldots, N\} \to \{1, \ldots, N\}$,*

$$(x_1, \ldots, x_N) \in U_d \implies (x_{\pi(1)}, \ldots, x_{\pi(N)}) \in U_d.$$

In the next theorem, we show an algebraic property of $\mathcal{T}_d$.

THEOREM 4.3. *Let d be an N-admissible real number. The pair $(\mathcal{T}_d, +)$ is a normal subgroup of $(\mathbb{Z}^N, +)$.*

PROOF. Since $(\mathbb{Z}^N, +)$ is an Abelian group, we only need to check that $(\mathcal{T}_d, +)$ is a subgroup of $(\mathbb{Z}^N, +)$. Take x and y from $\mathcal{T}_d$. In order to prove the theorem, it suffices to show that $x - y \in \mathcal{T}_d$. There are d-walks

$$\mathcal{U}_1 = \{u_1, \ldots, u_k\} \quad \text{and} \quad \mathcal{U}_2 = \{v_1, \ldots, v_m\}$$

from the origin to x and y, respectively. Consider the d-walk

$$\mathcal{U} = \{u_1, \ldots, u_k, u_{k+1}, \ldots, u_{k+m}\},$$

where $u_{k+i} = -v_i$ for $i = 1, \ldots, m$. Clearly, $\mathcal{U}$ is a d-walk from the origin to $x - y$. Thus $x - y \in \mathcal{T}_d$ and the proof is complete. $\square$

We say that $L \subset \mathbb{Z}^N$ is a *sublattice* of $\mathbb{Z}^N$ if L is an additive subgroup and the vector space spanned by L is $\mathbb{R}^N$. From the abovementioned geometric properties of $\mathcal{T}_d$, Proposition 4.2 and Theorem 4.3, we get the following corollary.

COROLLARY 4.4. *Let d be an N-admissible real number. Then $\mathcal{T}_d$ is a sublattice of $\mathbb{Z}^N$.*

Let $u_1, \ldots, u_N \in \mathbb{Z}^N$ be linearly independent vectors in $\mathbb{R}^N$. The sublattice L of $\mathbb{Z}^N$ generated by $u_1, \ldots, u_N$ is defined as

$$L = \left\{ \sum_{i=1}^{N} a_i u_i : a_i \in \mathbb{Z}, i = 1, \ldots, N \right\}.$$

The fundamental parallelepiped of L is the set

$$\Pi_L = \left\{ \sum_{i=1}^{N} t_i u_i : 0 \le t_i < 1, i = 1, \ldots, N \right\}.$$

The next lemma is similar to [4, Theorem 2.3.12] and can be proved in an analogous way.

LEMMA 4.5. *Let L be a sublattice of $\mathbb{Z}^N$ generated by $u_1, \ldots, u_N$. Then, for any $w \in \mathbb{Z}^N$, the coset $w + L$ coincides with a coset $w_0 + L$ for some $w_0 \in \Pi_L \cap \mathbb{Z}^N$. Moreover, if w_1 and w_2 are two distinct points in $\Pi_L \cap \mathbb{Z}^N$, then $(w_1 + L) \cap (w_2 + L) = \emptyset$.*

An immediate consequence of Lemma 4.5 is the following corollary.

COROLLARY 4.6. *Let L be a sublattice of $\mathbb{Z}^N$ generated by $u_1, \ldots, u_N \in \mathbb{Z}^N$. Then*

$$|\mathbb{Z}^N / L| = |\Pi_L \cap \mathbb{Z}^N|.$$

5. The cardinality of $\mathbb{Z}^2 / \mathcal{T}_d$

After observing Theorem 4.3, it is natural to deal with the quotient $\mathbb{Z}^N / \mathcal{T}_d$, which will be the main object of the remaining part of this note. We start with two useful lemmas, the first of which immediately follows from [7, Theorem 4.1].

LEMMA 5.1. *Let d be a 2-reduced real number such that d^2 is an odd number. Then $\mathcal{T}_d = \mathbb{Z}^2$.*

LEMMA 5.2. *Let d be a 2-reduced real number such that d^2 is even. Then $\mathcal{T}_d \ne \mathbb{Z}^2$ and $\mathcal{T}_d$ is a sublattice of $\mathbb{Z}^2$ generated by the vectors $(1, 1)$ and $(-1, 1)$.*

PROOF. Assume that d is a 2-reduced real number such that d^2 is even. From the proof of [7, Theorem 4.1], it follows that $(1, 0) \notin \mathcal{T}_d$ and hence $\mathcal{T}_d \ne \mathbb{Z}^2$. In view of Corollary 4.4, it is enough to show that the vectors $(1, 1)$ and $(-1, 1)$ belong to $\mathcal{T}_d$. As $\mathcal{T}_d$ is symmetrical with respect to the y-axis, we only show that $(1, 1) \in \mathcal{T}_d$.

From the assumption that d is 2-reduced, it follows that there exists a vector $v_1 = (x_1, x_2) \in U_d$ with $\gcd(x_1, x_2) = 1$. Of course, we may assume that $0 < x_1 < x_2$. Consider the subset $U_d^0 \subset U_d$ consisting of v_1, $v_2 = (-x_2, x_1)$, $v_3 = (x_2, x_1)$ and $v_4 = (-x_1, x_2)$. We shall show that there exists a lattice walk from the origin to the point $(1, 1)$ using steps from the set $U_d^0 \cup (-U_d^0)$. The existence of such a walk will be clear if we show that the system of linear equations

$$\begin{cases} 1 = a_1 x_1 - a_2 x_2 + a_3 x_2 - a_4 x_1, \\ 1 = a_1 x_2 + a_2 x_1 + a_3 x_1 + a_4 x_2, \end{cases} \tag{5.1}$$

has an integral solution a_1, a_2, a_3 and a_4. By substituting $\alpha = a_1 - a_4$, $\beta = a_3 - a_2$, $\gamma = a_3 + a_2$ and $\delta = a_1 + a_4$, the system (5.1) gives

$$\begin{cases} 1 = \alpha x_1 + \beta x_2, \\ 1 = \gamma x_1 + \delta x_2. \end{cases} \tag{5.2}$$

Since $\gcd(x_1, x_2) = 1$, both equations in (5.2) have the same integral solution α_0 and β_0. All other solutions of (5.2) are given by

$$\alpha = \alpha_0 + x_2 t, \quad \beta = \beta_0 - x_1 t, \quad \gamma = \alpha_0 + x_2 s \quad \text{and} \quad \delta = \beta_0 - x_1 s,$$

where t, s are arbitrary integers.

Using this, and returning to the original unknowns a_1, a_2, a_3 and a_4, yields

$$\begin{cases} a_1 - a_4 = \alpha_0 + x_2 t, \\ a_1 + a_4 = \beta_0 - x_1 s. \end{cases} \quad \text{and} \quad \begin{cases} a_3 - a_2 = \beta_0 - x_1 t, \\ a_3 + a_2 = \alpha_0 + x_2 s. \end{cases}$$

Solving the two systems, we easily obtain

$$a_1 = \frac{\alpha_0 + \beta_0 - x_1 s + x_2 t}{2}, \quad a_4 = a_1 - (\alpha_0 + x_2 t) \tag{5.3}$$

and

$$a_3 = \frac{\alpha_0 + \beta_0 - x_1 t + x_2 s}{2}, \quad a_2 = a_3 + (x_1 t - \beta_0). \tag{5.4}$$

It remains now to show that, for suitable integers t and s, all four unknowns are integers. In view of (5.3) and (5.4), it is enough to ensure that a_1 and a_3 are integers.

From the assumptions that d is 2-reduced and d^2 is even, it follows that both the numbers x_1 and x_2 are odd. From this and the equality $\alpha_0 x_1 + \beta_0 x_2 = 1$ it follows, in turn, that α_0 and β_0 must be of different parity. It is easy to check that when we put $s = \alpha_0$ and $t = \beta_0$, then a_1 and a_3 are integers. Hence all four unknowns are integers and this completes the proof. □

Now we are ready to establish the main result of this section and the paper.

THEOREM 5.3. *Let d be a* 2-*admissible real number. Then*

$$|\mathbb{Z}^2 / \mathcal{T}_d| = \begin{cases} h_d^2 & \text{when } (d/h_d)^2 \text{ is odd,} \\ 2h_d^2 & \text{when } (d/h_d)^2 \text{ is even.} \end{cases}$$

PROOF. Take a 2-admissible real number d. From (2.1) and the form of h_d, it follows that $(d/h_d)^2$ is either odd (when $\alpha = 0$) or even (when $\alpha = 1$). We will consider the two possible cases separately.

Case $\alpha = 0$: By Lemma 5.1, the terminal set $\mathcal{T}_{d/h_d}$ is just $\mathbb{Z}^2$. From Corollaries 4.4 and 4.1, it follows that $\mathcal{T}_d$ is a sublattice of $\mathbb{Z}^2$ generated by the vectors $u_1 = (h_d, 0)$ and $u_2 = (0, h_d)$. Clearly, $\Pi_{\mathcal{T}_d}$ contains h_d^2 lattice points. This, in conjunction with Corollary 4.6, ends the proof in this case.

Case $\alpha = 1$: By Lemma 5.2 and Corollaries 4.4 and 4.1, $\mathcal{T}_d$ is a sublattice of $\mathbb{Z}^2$ generated by the vectors $u_1 = (h_d, h_d)$ and $u_2 = (-h_d, h_d)$. One can easily check that, in this case, $\Pi_{\mathcal{T}_d}$ contains $2(h_d)^2$ lattice points. By Corollary 4.6, $|\mathbb{Z}^2 / \mathcal{T}_d| = 2(h_d)^2$, which establishes the case when $\alpha = 1$. The proof of the theorem is complete. □

6. A problem about the cardinality of $\mathbb{Z}^N/\mathcal{T}_d$

Corollary 4.6, in conjunction with Corollary 4.4, provides some kind of implicit information about the cardinality of $\mathbb{Z}^N/\mathcal{T}_d$. It would be interesting to find an explicit formula for $|\mathbb{Z}^N/\mathcal{T}_d|$ depending on d and N in a similar way to the formula in Theorem 5.3. Therefore we formulate the following problem.

PROBLEM 6.1. Let d be an N-admissible real number. Express the cardinality of $\mathbb{Z}^N/\mathcal{T}_d$ in terms of d and N.

Acknowledgement

References

[1] C. Banderier and Ph. Flajolet, 'Basic analytic combinatorics of directed lattice paths', *Theoret. Comput. Sci.* **281** (2002), 37–80.

[2] D. M. Burton, *Elementary Number Theory* (McGraw-Hill, Boston, 2002).

[3] V. Dabbagian-Abdoly, 'On the enumeration of higher dimensional lattice paths', *Int. J. Pure Appl. Math.* **23** (2005), 475–477.

[4] J. A. De Loera, R. Hemmecke and M. Köppe, *Algebraic and Geometric Ideas in the Theory of Discrete Optimization*, MOS-SIAM Series on Optimization (SIAM, Philadelphia, 2013).

[5] L. E. Dickson, *History of the Theory of Numbers, Vol. 2* (Carnegie Institution of Washington, 1920), republished by Dover, New York, 2005.

[6] I. Jensen, 'Enumeration of self-avoiding walks on the square lattice', *J. Phys. A* **37** (2004), 5503–5524.

[7] K. Kołodziejczyk, 'Parity properties and terminal points for lattice walks with steps of equal length', *J. Math. Anal. Appl.* **35** (2009), 363–368.

[8] W. Sierpiński, 'Sur les nombres impairs admettant une seule décomposition en une somme de deux carrés de nombres naturels premiers entre eux', *Elem. Math.* **16** (1961), 27–30.

[9] W. Sierpiński, *Elementary Theory of Numbers* (ed. A. Schinzel) (North-Holland, Amsterdam, 1988).

[10] U. Tamm, 'Lattice paths not touching a given boundary', *J. Statist. Plann. Inference* **105** (2002), 433–448.

[11] W.-J. Woan, 'Diagonal lattice paths', *Congr. Numer.* **151** (2001), 173–178.

KRZYSZTOF KOŁODZIEJCZYK, Faculty of Pure and Applied Mathematics,
Wrocław University of Science and Technology,
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
e-mail: krzysztof.kolodziejczyk@pwr.edu.pl

RAFAŁ SAŁAPATA, Faculty of Pure and Applied Mathematics,
Wrocław University of Science and Technology,
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
e-mail: rafal.salapata@pwr.edu.pl