REPRESENTING GENERALIZED DERANGEMENTS AS SUMS OF THREE SQUARES

MACIEJ ULAS

Abstract. Let $D_n^{(v)}$ be the nth generalized derangement number that is a generalization of the classic derangement number $D_n = D_n^{(0)}$. In this note, we investigate the set S_v of those integers n for which $D_n^{(v)}$ is not a sum of three squares. We characterize the set S_0 and the set S_v for odd values of v. We prove that in these cases the set S_v has natural density and compute its value. In particular, the natural density of S_0 is equal to $1/24$.

1. Introduction

Let $\mathbb{N}$ be the set of nonnegative integers, $\mathbb{N}_+$ the set of positive integers, and for a given $k \in \mathbb{N}_+$, let $\mathbb{N}_{\geq k} = \{n \in \mathbb{N} : n \geq k\}$. Moreover, by $\nu_2(n)$ we denote the 2-adic valuation of an integer n; i.e., the largest $k \in \mathbb{N}$ such that $2^k | n$ (with the convention $\nu_2(0) = +\infty$).

One of the classic theorems of arithmetic theory of quadratic forms is the characterization of integers that can be represented as a sum of three squares of integers. The result, proved by Legendre in 1798, states that the Diophantine equation

$$n = x^2 + y^2 + z^2,$$

where n is positive integer, has no solution in integers x, y, z if and only if n is of the form $n = 2^{2k}(8m + 7)$. Thus, the question concerning the representation of n as a sum of three squares is reduced to the study of 2-adic valuation of n, with the modulo 8 behavior of $n/2^{\nu_2(n)}$ (in the case when $\nu_2(n)$ is even). This approach was successfully adapted in the study of various Diophantine equations of the form

$$u_n = x^2 + y^2 + z^2, \tag{1.1}$$

where $(u_n)_{n\in\mathbb{N}}$ is an integer sequence of a combinatorial origin. For example, Granville and Zhu presented the characterization of those n for which equation (1.1) with $u_n = \binom{2n}{n}$ has a solution (note that some initial results concerning this case were also obtained by Robbins in [7]). The same approach was used in a recent study of Deshouillers and Luca concerning the solvability of (1.1) with $u_n = n!$ [1]. In this case, one can also consult a recent paper of Hajdu and Papp [3], where the question concerning the so called gap sequences is investigated.

The numbers $\binom{2n}{n}$ and $n!$ have a natural combinatorial interpretation and it is interesting to ask for which numbers with a combinatorial origin, similar results can be obtained. In this note, we continue this line of research and consider the equation (1.1) with $u_n = D_n^{(v)}$. Here, for $v \in \mathbb{N}$, the number $D_n^{(v)}$ is the so called generalized derangement number. More precisely, for fixed $v \in \mathbb{N}$ and $n \in \mathbb{N}$, the nth generalized derangement number $D_n^{(v)}$ is defined by (see

The research of the author is supported by the grant of the National Science Centre (NCN), Poland, no. UMO-2019/34/E/ST1/00094.

Munarini [6])

$$D_n^{(v)} = \sum_{k=0}^{n} (-1)^k \binom{v+n-k}{n-k} \frac{n!}{k!}.$$

We prefer the notation $D_n^{(v)}$ instead of Munarini's $d_n^{(v)}$ to strengthen the connection with the classic derangement numbers, which are the special case for $v = 0$. Arithmetic properties of these numbers were investigated from different perspectives (e.g., the recent paper [10] and reference given there). In general, for a given $v \in \mathbb{N}$, the number $D_n^{(v)}$ is the permanent of the $(0, 1)$-matrix of size $n \times (n + v)$ with n zeros not on a line. For various values of v, the number $D_n^{(v)}$ has an additional combinatorial interpretation. Recall that $D_n^{(0)}$ is the number of the permutations of the set $\{1, \ldots, n\}$ without fixed points - the classic derangement number or *rencontres numbers* was introduced and studied by Montmort [5] (for a large number of interpretations of these numbers, see entry A000166 in [8]). For $v = 1$, the number $D_n^{(1)}$ counts permutations of the set $\{1, \ldots, n+1\}$ having no substrings of the form $(k, k+1)$ for any $k \in \{1, \ldots, n\}$. The number $D_n^{(2)}$ counts certain type of necklaces (for a precise description, see the entry A000153 in [8]) and so on.

One can easily check that $D_0^{(v)} = 1$, $D_1^{(v)} = v$, and for $n \geq 2$, we have

$$D_n^{(v)} = (n + v - 1)D_{n-1}^{(v)} + (n - 1)D_{n-2}^{(v)}. \tag{1.2}$$

Moreover, we have the identity that connects the value of $D_n^{(v)}$ with $D_n^{(v-1)}$; i.e.,

$$D_n^{(v)} = nD_{n-1}^{(v)} + D_n^{(v-1)}.$$

Motivated by findings from the papers [1, 2], we study the set

$$S_v := \{n \in \mathbb{N} : \ D_n^{(v)} \text{ is not a sum of three squares of integers}\}$$

and the counting function

$$S_v(x) = \#\{n : \ n \leq x \text{ and } n \in S_v\}.$$

Let us describe the content of the paper in some detail. In Section 2, we obtain a precise description of the elements of the set S_0. Using this characterization of S_0, we compute $S_0(x)$ with error of logarithmic growth and prove that the natural density of S_0 in $\mathbb{N}$ is equal to $1/24$. In Section 3, we describe the elements of the set S_v for $v \equiv 1 \pmod 2$ and compute the natural density. In the last section, we speculate on possible solutions of more difficult problems concerning the representability of $D_n^{(0)}$ as a sum of two squares or as a sum of two squares and a fourth power.

2. Characterization of the Elements of the Set S_0

We start our investigations with the case $v = 0$. To simplify the notation, we write D_n instead of $D_n^{(0)}$. Recall that D_n is the number of permutations of the set $\{1, \ldots, n\}$ without fixed points. By a simple combinatorial argument, one can check that the sequence $(D_n)_{n \in \mathbb{N}}$ satisfies the following recurrence

$$D_0 = 1, \ D_n = nD_{n-1} + (-1)^n \text{ for } n \in \mathbb{N}_+. \tag{2.1}$$

Using recurrence (2.1) two times, we get an additional recurrence relation in the following form

$$D_0 = 1, \ D_1 = 0, \ D_n = (n - 1)(D_{n-1} + D_{n-2}) \quad \text{for} \quad n \in \mathbb{N}_{\geq 2}, \tag{2.2}$$

which also follows from (1.2) by taking $v = 0$.

We start with the following lemma.

Lemma 2.1. *We have the following congruences:*

$$D_{2n} \equiv 1 \pmod 8 \quad \text{and} \quad D_{2n+1} \equiv 2n \pmod 8.$$

Proof. First, note that recurrence (2.1) implies the recurrence $D_{2n} = 2n(2n-1)D_{2(n-1)}+1-2n$. We have $D_0 = D_2 \equiv 1 \pmod 8$, and by induction on n, we get

$$D_{2n} \equiv 2n(2n-1)D_{2(n-1)} + 1 - 2n \equiv 2n(2n-1) + 1 - 2n \equiv 4n(n-1) + 1 \equiv 1 \pmod 8.$$

The first congruence follows.

The second congruence is an immediate consequence of the first one. Indeed, we have

$$D_{2n+1} = (2n+1)D_{2n} - 1 \equiv 2n + 1 - 1 \equiv 2n \pmod 8,$$

and we get the statement. □

To obtain the characterization of the elements in S_0, we also need the following characterization of the 2-adic valuation of D_n.

Lemma 2.2. *For $n \in \mathbb{N}$, we have $\nu_2(D_n) = \nu_2(n-1)$.*

Proof. For $n = 0, 1, 2$, the statement is true. From recurrence (2.2) and Lemma 2.1, we have that

$$\nu_2(D_n) = \nu_2((n-1)(D_{n-1} + D_{n-2})) = \nu_2(n-1) + \nu_2(D_{n-1} + D_{n-2}) = \nu_2(n-1).$$

□

We characterize the behavior of $D_n/2^{\nu_2(n-1)}$ modulo 8 in the following result.

Theorem 2.3. *Let $n \in \mathbb{N}$ and write $n = 2^k(2m+1)+1$ for some $k, m \in \mathbb{N}$. Then,*

$$\frac{D_n}{2^{\nu_2(n-1)}} = \frac{D_{2^k(2m+1)+1}}{2^k} \equiv \begin{cases} 1 \pmod 8 & \text{for } k = 0, \\ 1 - 2m \pmod 8 & \text{for } k = 1, \\ 3 - 2m \pmod 8 & \text{for } k = 2, \\ 7 - 2m \pmod 8 & \text{for } k \geq 3. \end{cases}$$

Proof. The case $k = 0$ is already proved in Lemma 2.1. We thus assume that $k \geq 1$. From recurrence (2.2) and Lemma 2.1, we get that

$$\begin{aligned} \frac{D_{2^k(2m+1)+1}}{2^k} &= (2m+1)(D_{2^k(2m+1)} + D_{2^k(2m+1)-1}) \\ &\equiv (2m+1)(D_{2(2^k m + 2^{k-1} - 1)+1} + 1) \pmod 8 \\ &\equiv \begin{cases} (2m+1)(D_{4m+1} + 1) \pmod 8 & \text{for } k = 1, \\ (2m+1)(D_{2(4m+1)+1} + 1) \pmod 8 & \text{for } k = 2, \\ (2m+1)(D_{2(2^{k-1}(2m+1)-1)+1} + 1) \pmod 8 & \text{for } k \geq 3 \end{cases} \\ &\equiv \begin{cases} (2m+1)(4m+1) \pmod 8 & \text{for } k = 1, \\ (2m+1)(2(4m+1)+1) \pmod 8 & \text{for } k = 2, \\ (2m+1)(2^k(2m+1)-1) \pmod 8 & \text{for } k \geq 3 \end{cases} \\ &\equiv \begin{cases} 1 - 2m \pmod 8 & \text{for } k = 1, \\ 3 - 2m \pmod 8 & \text{for } k = 2, \\ 7 - 2m \pmod 8 & \text{for } k \geq 3; \end{cases} \end{aligned}$$

and the result follows. □

As a consequence, we get the following theorem.

Theorem 2.4. *Let $n \in \mathbb{N}$. We have the following equivalence:*

$$n \in S_0 \iff n = 32s + 21 \text{ or } n = 2^{2k+3}s + 2^{2k} + 1$$

for some $s \in \mathbb{N}$ and $k \in \mathbb{N}_{\geq 2}$.

Proof. From Legendre's theorem, we know that $n \in S_0$ if and only if $\nu_2(D_n) = \nu_2(n-1) \equiv 0 \pmod 2$ and $D_n/2^{\nu_2(n-1)} \equiv 7 \pmod 8$. Thus, from Theorem 2.3, we get:

(1) $n = 4(2m+1) + 1$ and $3 - 2m \equiv 7 \pmod 8$; or
(2) $n = 2^{2k}(2m+1) + 1$ and $7 - 2m \equiv 7 \pmod 8$.

In the first case, we get $m \equiv 2 \pmod 4$; i.e., $m = 4s + 2$. Hence, $n = 8m + 5 = 32s + 21$.

In the second case, we get $m \equiv 0 \pmod 4$; i.e., $m = 4s$. Hence, $n = 2^{2k}(8s+1) + 1$. Our result follows.

□

The above characterization allows us to get precise information concerning the behavior of $S_0(x)$. More precisely, we are able to prove the following result.

Corollary 2.5. *We have the equality*

$$S_0(x) = \frac{1}{24}x + O(\log_2 x).$$

In particular, the natural density of the set S_0 in $\mathbb{N}$ is equal to

$$\text{dens}(S_0) = \lim_{x \to +\infty} \frac{S_0(x)}{x} = \frac{1}{24}.$$

Proof. Using the characterization of the set S_0 given in Theorem 2.4, we get the following chain of equalities:

$$\begin{aligned} S_0(x) =& \#\{n \leq x : \ n = 32s + 21, \ s \in \mathbb{N}\} \\ &+ \#\{n \leq x : \ n = 2^{2k}(8s+1) + 1, \ s \in \mathbb{N}_+, k \in \mathbb{N}_{\geq 2}\} \\ =& \frac{x}{32} + O(1) + \sum_{k=2}^{\log_2 x} \left(\frac{x}{2^{2k+3}} + O(1) \right) \\ =& \frac{x}{32} + \frac{x}{96} + O(\log_2 x) = \frac{x}{24} + O(\log_2 x). \end{aligned}$$

The second property from the statement is immediate. □

3. Characterization of the Elements of the Set S_v for v Odd

Let $v = 2m+1$ for some $m \in \mathbb{N}$. We start with a lemma that shows it is enough to consider $D_n^{(v \pmod 8)}$. More precisely, we have the following lemma.

Lemma 3.1. *For given $v \in \mathbb{N}$ and each $n \in \mathbb{N}$ we have*

$$D_n^{(v+8)} \equiv D_n^{(v)} \pmod 8.$$

If v is also an odd integer, then for each $n \in \mathbb{N}$, the number $D_n^{(v)}$ is odd. In this particular case, we have the equality of sets $S_v = S_{v \pmod 8}$.

Proof. The first statement is true for $n = 0$ because $D_0^{(v)} = 1$ for each v. For $n = 1$, we have $D_1^{(v+8)} - D_1^{(v)} = v + 8 - v = 8 \equiv 0 \pmod 8$. Let us assume that it is true for $n - 1$ and $n - 2$. Then, from the recurrence relation satisfied by $D_n^{(v)}$ and the induction hypothesis, we get

$$D_n^{(v+8)} - D_n^{(v)} \equiv (n + v - 1)(D_{n-1}^{(v+8)} - D_{n-1}^{(v)}) + (n - 1)(D_{n-2}^{(v+8)} - D_{n-2}^{(v)}) \equiv 0 \pmod 8,$$

and our result follows.

Assume that v is odd and recall that $D_0^{(v)} = 1$ and $D_1^{(v)} = v$. It is clear that these integers are odd. Next, for $n \geq 2$ we have $D_n^{(v)} = (n + v - 1)D_{n-1}^{(v)} + (n - 1)D_{n-2}^{(v)}$ and assuming that our statement is true for $n - 1$ and $n - 2$ and using induction on n, we have

$$D_n^{(v)} \equiv nD_{n-1}^{(v)} + (n - 1)D_{n-2}^{(v)} \equiv 2n - 1 \equiv 1 \pmod 2,$$

and our result follows. □

Having the above properties at our disposal, we prove the following theorem.

Theorem 3.2. *For a given $m \in \mathbb{N}$ and $n \in \mathbb{N}$ the following congruences are true:*

$$D_n^{(8m+1)} \equiv 2\left\lfloor \frac{n}{2} \right\rfloor + 1 \pmod 8;$$

$$D_n^{(8m+3)} \equiv D_{2n}^{(8m+1)} \equiv 2n + 1 \pmod 8;$$

$$D_n^{(8m+5)} \equiv \begin{cases} 1 & \text{for } n \equiv 0, 5 \pmod 8, \\ 3 & \text{for } n \equiv 3, 6 \pmod 8, \\ 5 & \text{for } n \equiv 1, 4 \pmod 8, \\ 7 & \text{for } n \equiv 2, 7 \pmod 8; \end{cases}$$

$$D_n^{(8m+7)} \equiv 6(n \pmod 2) + 1 \pmod 8.$$

Proof. In each case, the proof of the expression for $D_n^{(v)} \pmod 8$ given in the statement is a simple application of Theorem 3.1 and induction on n. Because the proofs go in exactly the same way, we present the details only in the case when $v \equiv 1 \pmod 8$.

If $v \equiv 1 \pmod 8$, then from Theorem 3.1, we get that for each n the congruence $D_n^{(v)} \equiv D_n^{(1)} \pmod 8$ is true. Next, using induction on n, we easily get $D_n^{(1)} \equiv 2\left\lfloor \frac{n}{2} \right\rfloor + 1 \pmod 8$ and hence, the result. □

As an immediate application of Theorem 3.2, we get the following corollary.

Corollary 3.3. *For an odd integer v, we have $S_v = S_{v \pmod 8}$. Moreover, we have the following equalities of sets:*

$$S_1 = \{n \in \mathbb{N} : \ n \equiv 6, 7 \pmod 8\},$$
$$S_3 = \{n \in \mathbb{N} : \ n \equiv 3 \pmod 4\},$$
$$S_5 = \{n \in \mathbb{N} : \ n \equiv 2, 7 \pmod 8\},$$
$$S_7 = \{n \in \mathbb{N} : \ n \equiv 1 \pmod 2\},$$

and the densities

$$\operatorname{dens}(S_v) = \lim_{x \to +\infty} \frac{S_v(x)}{x} = \begin{cases} 1/4 & \text{for } v \equiv 1, 3, 5 \pmod 8; \\ 1/2 & \text{for } v \equiv 7 \pmod 8. \end{cases}$$

Proof. Because for an odd value of v, the number $D_n^{(v)}$ is odd, the equality of sets follow from the congruence $D_n^{(v+8)} \equiv D_n^{(v)} \pmod{8}$ (Lemma 3.1).

The description of the set S_v for $v = 1, 3, 5, 7$ is equivalent with the study of solutions (in variable n) of the congruence $D_n^{(v)} \equiv 7 \pmod{8}$. This form is an immediate consequence of Theorem 3.2. Finally, having the characterization of elements of the set S_v, we easily obtain that $S_v(x) = x/4 + O(1)$ for $v \equiv 1, 3, 5 \pmod{8}$ and $S_v(x) = x/2 + O(1)$ for $v \equiv 7 \pmod{8}$. Applying these equalities, we get the values of the corresponding densities. □

4. Computational Observations, Questions, and A Conjecture

From our investigations in the previous section, the following problem is the most interesting.

Problem 4.1. *Let v be even. Characterize the elements of the set $S_v = \{n \in \mathbb{N} : D_n^{(v)}$ is not the sum of three squares$\}$.*

It is not difficult to prove that for each even v, the set S_v is infinite. More precisely, we have the following congruences

$$D_{8n+2}^{(8m+2)} \equiv D_{8n+6}^{(8m+6)} \equiv 7 \pmod{8}.$$

Thus, $8n + 2 \in S_{8m+2}$ and $8n + 6 \in S_{8m+6}$. We thus see that if $v \equiv 2 \pmod{4}$ and S_v has a density, then $\operatorname{dens}(S_v) \geq 1/8$. Similarly, we have

$$D_{32n+p_i}^{(4m)} \equiv 28 \pmod{32},$$

where $m \equiv i \pmod{8}$ and

$$(p_0, \dots, p_7) = (21, 9, 29, 17, 5, 25, 13, 1).$$

These congruences imply that if $v \equiv 0 \pmod{4}$ and S_v has a density, then $\operatorname{dens}(S_v) \geq 1/32$. One can also check that for $v = 2m$, and for each $n \in \mathbb{N}$ and $i \in \{0, 2, 3\}$, the following noncongruence holds:

$$D_{4n+2(m \pmod{2})+i}^{(2m)} \not\equiv 0 \pmod{4}.$$

Performing analysis similar to the one presented in Section 3, it is possible to obtain those values of n such that $D_{4n+2(m \pmod{2})+i}^{(2m)} \equiv 7 \pmod{8}$; i.e., we have $4n+2(m \pmod{2})+i \in S_v$. However, we were unable to compute the 2-adic valuation of the number $D_{4n+2(m \pmod{2})+1}^{(2m)}$ and numeric computations suggest that for each m, we have $\nu_2(D_{4n+2(m \pmod{2})+1}^{(2m)}) \to +\infty$ with n. This suggests the following problem.

Problem 4.2. *Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Compute the value of $\nu_2(D_{4n+2(m \pmod{2})+1}^{(2m)})$.*

For $v = 0$ or v odd, we obtained the existence (and the value) of $\operatorname{dens}(S_v)$. A natural question arises whether it is possible to prove the existence of the density of S_v for v even without characterizing the elements of the set S_v. We thus formulate the following question.

Question 4.3. *Let v be even positive integer. Does the natural density of S_v exist?*

In light of a result obtained in Section 2, one can ask related questions about the existence of representations of $D_n = D_n^{(0)}$ by sums of even powers. It is clear that the same type of questions can be asked for any $v \in \mathbb{N}_+$.

First, let

$$T := \{n \in \mathbb{N} : \ D_n \text{ is a sum of two squares of integers}\}.$$

It is clear that $T \subset \mathbb{N} \setminus S_0$. Recall that a positive integer m can be written as a sum of two squares if and only if prime numbers p such that $p|m$ and $p \equiv 3 \pmod 4$ appear in the factorization of m with even powers. However, as we know, the number D_n grows quickly with n. Indeed, the number of digits of D_n is around $n \log n$ and it is a nontrivial problem to check whether $n \in T$. We checked that there are at least 22 elements of the set T that are ≤ 200. They are the following:

$$1, 2, 3, 4, 6, 10, 11, 12, 13, 14, 18, 26, 30, 34, 38, 62, 66, 74, 89, 118, 131, 138.$$

In the range under consideration, there are five values of n for which we have not been able to check whether n is in T or not. They are the following: $147, 177, 184, 188, 193$. The reason is simple. There is no quick way to check whether a large composite integer is the sum of two squares without factoring it (in the case of a prime number, the situation is better - see for example [9]). In each of the problematic cases, the number D_n contains a composite co-factor with more than 200 digits, which we have not been able to factor. This explains the difficulty in obtaining larger elements of T. For example, we know that $74 \in T$ and this follows from the factorization $D_{74} = 73pq$, where

$$p = 532202503414385269441033, \quad q = 30384550713083856285289293474527653.$$

Here, p and q are primes with 24 and 35 digits respectively. Moreover, to show that $144 \notin T$, a 30 digit prime factor $p = 262818855883805693639763176627$ of the 232 digit number $D_{144}/(11 \cdot 143 \cdot 848804537899393)$ was found.

In light of our computations, we formulate the following question.

Question 4.4. *Is the set T infinite?*

We believe that the answer to this question is YES, but it seems that proving such a result is difficult. On the other hand, it is not difficult to prove that the set $\mathbb{N} \setminus T$ is infinite. Let $p \equiv 3 \pmod 4$ be a prime and suppose that $p||n-1$. If additionally $p \nmid D_{n-1} + D_{n+1}$, then $\nu_p(D_n) = 1$ and the number D_n cannot be a sum of two squares. Equivalently, because $p|n-1$ and $D_{n-1} \equiv (-1)^{n-1} D_0 \pmod{n-1}$, we get that $D_{n-1} \equiv (-1)^{n-1} \pmod p$. Similar reasoning reveals that $D_{n-2} \equiv (-1)^{n-2-(p-1)} D_{p-1} \pmod{n-2-(p-1)}$ and thus, $D_{n-2} \equiv (-1)^n \pmod p$. We thus see that our n satisfies $n \notin T$ provided p does not divide $D_{p-1} - 1$. Let p_m be the mth prime. We checked that the congruence $D_{p_m - 1} \equiv 1 \pmod{p_m}$ has only two solutions $p_2 = 3$ and $p_5 = 11$ for $m \leq 20000$, and we can produce many arithmetic progression of numbers not in T. Although limited, our computations strongly suggest that the natural density of the set $\mathbb{N} \setminus T$ is 1. To show that $\mathbb{N} \setminus T$ is infinite, we take $p = 7$. Then, for each $k \in \mathbb{N}$ and $i \in \{1, \ldots, 6\}$, the number $n = 49k + 7i + 1$ has the property that $\nu_7(D_n) = 1$ and hence, $n \notin T$.

However, here is a heuristic reasoning provided by the referee that supports the belief that the set T is infinite. It is known, by Landau's result, that the number of integers n such that $n \leq x$ and n is a sum of two squares of integers is $\sim c_0 x / \sqrt{\log x}$, with some positive constant c_0. So, one can say that "the probability" that a positive integer n is a sum of two squares is around $c_1/\sqrt{\log n}$ for some constant c_1. Because

$$D_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!},$$

we can apply Stirling's formula for $n!$ and get that $\sqrt{\log D_n} = (1+o(1))\sqrt{n\log n}$. Thus, one can expect that the expectation that D_n is a sum of two squares is $c_1/\sqrt{n\log n}$. However, this expectation is probably smaller because $n-1|D_n$ and the $\gcd(n-1, D_{n-1}+D_{n-2})$ is not divisible by a prime $p\equiv 3 \pmod 4$. So, if D_n is a sum of two squares, then $n-1$ and $D_{n-1}+D_{n-2}$ should be almost sums of two squares in the sense that there is a small square-free number d, divisible only by primes $q\equiv 3 \pmod 4$, such that $D_{q-1}\equiv 1 \pmod q$ and that $n-1 = d(x_1^2+x_2^2)$ and $D_{n-1}+D_{n-2} = d(y_1^2+y_2^2)$. Assuming that these events are independent, one may expect the probability that D_n is a sum of two squares is equal to $c_2/(\sqrt{n}\log n)$ for some positive constant c_2. As a consequence, we would get that the number of $n\in T$ up to x is

$$\sum_{n\le x}\frac{1}{\sqrt{n}\log n} \asymp (2+o(1))\frac{\sqrt{x}}{\log x}.$$

This means that T is likely to be infinite and contains $x^{1/2-o(1)}$ integers $n\le x$ as x tends to infinity.

We preformed some additional computations that suggest the expectation that D_n behaves like a random integer of the same size is a bit too optimistic. More precisely, in the discussed context, one can also ask what is the distribution of $D_n \pmod p$ for a given prime number p. Let us recall that for any given odd number m, the sequence $(D_n \pmod m)_{n\in\mathbb{N}}$ is periodic of period $2m$ [4, Proposition 1]. Due to the periodicity modulo p, it is enough to consider D_n for $n\le 2p-1$. It seems that the sequence $(D_n \pmod p)$ tends to avoid many residue classes. Let $p\le 93179 = p_{9000}$. We computed the number $r(p)$ of elements of the set

$$R(p) := \{D_n \pmod p:\ n\in\{0,\dots,2p-1\}\}.$$

In Figure 1, we can see the graphs of the functions $f(k) = p_k$ and $g(k) = r(p_k)$ for $k\le 9000$. The figure strongly suggest that $p_k - r(p_k)$ tends to infinity with k.

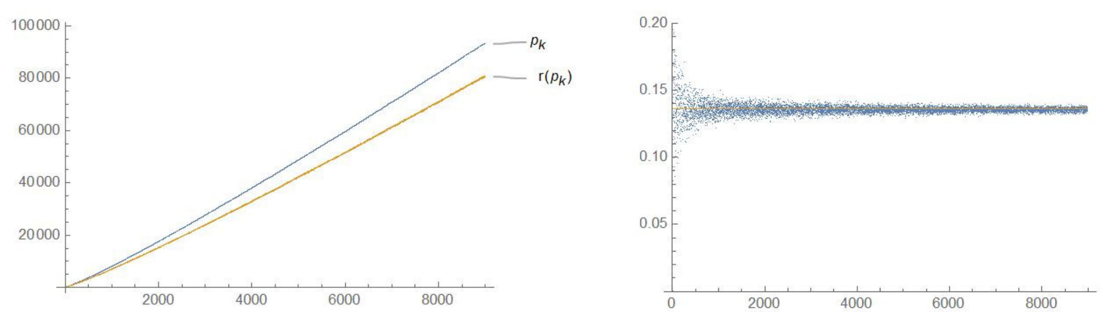

FIGURE 1. Plot of the functions $f(k) = p_k$ and $g(k) = r(p_k)$ (left) and the function $h(k) = (p_k - r(p_k))/r(p_k)$ (right) for $k\le 9000$.

One can also speculate whether the sequence of quotients $(r(p_k)/p_k)_{k\in\mathbb{N}}$ is convergent. Numeric calculations in the considered range confirmed that $r(p_k) > \frac{7}{11}p_k$. Moreover, it seems that for $k\ge 20$ we have $r(p_k) < \frac{23}{25}p_k$.

It seems that the set of values of the quotients $(p_k - r(p_k))/r(p_k)$ cluster around the horizontal line $y = 0.135997237$.

Now, let

$$Q := \{n\in\mathbb{N}:\ D_n \text{ is a sum of two squares and a fourth power}\}$$

It is clear that $T \subset Q$ and thus, $Q \subset \mathbb{N} \setminus S_0$. The problem whether $n \in Q$ is also a difficult one. Indeed, no characterization of integers that can be represented in the form $x^2 + y^2 + z^4$ without computing the representation somehow is known. On the other hand, we checked that for $n \in \mathbb{N} \setminus S_0$, $n \leq 50$, and $n \neq 5, 37$, we have $n \in Q$. More precisely, for each $n \neq 5, 37$, we were able to find a small value of z such that $D_n - z^4$ is a sum of two squares. The only representation of $D_5 = 44$ as a sum of three squares is $D_5 = 2^2 + 2^2 + 6^2$ and thus, D_5 is not a sum of two squares and a fourth power. We were unable to check whether D_{37} is a sum of two squares and a fourth power. We know that there is no $z \leq 10^6$ such that $D_{37} - z^4$ is a sum of two squares. Therefore, in the light of our computations, we formulate the following conjecture.

Conjecture 4.5. *The set Q is infinite and has a positive natural density in the set $\mathbb{N} \setminus S_0$.*

Acknowledgments

The author is grateful to an anonymous referee for several useful remarks, which led to improving the presentation.

References

[1] J.-M. Deshouillers and F. Luca, *How often is $n!$ a sum of three squares?* In: The Legacy of Alladi Ramakrishnan in the Mathematical Sciences, pages 243–251. Springer New York, 2010.
[2] A. Granville and Y. Zhu, *Representing binomial coefficients as sums of squares*, Amer. Math. Monthly, **97.6** (1990), 486–493.
[3] L. Hajdu and A. Papp, *On asymptotic density properties of the sequence $n!$*, Acta Arith., **184.4** (2018), 317–340.
[4] P. Miska, *Arithmetic properties of the sequence of derangements*, J. Number Theory, **163.6** (2016), 114–145.
[5] P. R. de Montmort, *Essai d'analyse sur les jeux de hasard*, Paris, 1708. Second edition published 1713–1714. Third edition reprinted in New York: Chelsea, pp. 131–138, 1980.
[6] E. Munarini, *Callan-like identities*, Online J. Anal. Comb., **14** (2019).
[7] N. Robbins, *Representing $\binom{2n}{n}$ as a sum of squares*, The Fibonacci Quarterly, **25.1** (1987), 29–33.
[8] N. J. A. Sloane, The on-line encyclopedia of integer sequences. Available at: `http://www.research.att.com/njas/sequences/`
[9] S. Wagon, *Editor's Corner: The Euclidean algorithm strikes again*, Amer. Math. Monthly, **97.2** (1990), 125–129.
[10] F.-Z. Zhao, *The log-balancedness of generalized derangement numbers*, Ramanujan Journal, **58** (2022), 121–129.

MSC2020: 11D09, 11D85

Faculty of Mathematics and Computer Science, Institute of Mathematics, Jagiellonian University, Łojasiewicza 6, 30 - 348 Kraków, Poland
Email address: `maciej.ulas@uj.edu.pl`