

RESEARCH

On the existence of magic squares of powers



Nick Rome¹ and Shuntaro Yamagishi^{2*} 

*Correspondence:
shuntaro.yamagishi@ist.ac.at
IST Austria, Am Campus 1, 3400
Klosterneuburg, Austria
Full list of author information is
available at the end of the article

Abstract

For any $d \geq 2$, we prove that there exists an integer $n_0(d)$ such that there exists an $n \times n$ magic square of d^{th} powers for all $n \geq n_0(d)$. In particular, we establish the existence of an $n \times n$ magic square of squares for all $n \geq 4$, which settles a conjecture of Várilly-Alvarado. All previous approaches had been based on constructive methods and the existence of $n \times n$ magic squares of d^{th} powers had only been known for sparse values of n . We prove our result by the Hardy-Littlewood circle method, which in this setting essentially reduces the problem to finding a sufficient number of disjoint linearly independent subsets of the columns of the coefficient matrix of the equations defining magic squares. We prove an optimal (up to a constant) lower bound for this quantity.

1 Introduction

Let $n \geq 1$ be an integer. A *magic square* is an $n \times n$ grid of distinct positive integers whose columns, rows, and two major diagonals all sum to the same number. The number to which all rows, columns and diagonals sum is known as the square's *magic constant*.

Magic squares have a long and rich history. Legend has it that the earliest recorded 3×3 magic square was first observed by Emperor Yu on the shell of a sacred turtle, which emerged from the waters of the Lo River [8, pp.118]. Since then magic squares have appeared in various cultures, and have been an object of curiosity in art, philosophy, religion and mathematics. The study of magic squares with additional structure is a topic that has garnered great interest in both recreational and research mathematics.

The first 4×4 magic square of squares (Figure 1) was constructed by Euler, in a letter sent to Lagrange in 1770. Though Euler did not provide any explanation of how he constructed the square, he presented his method to the St. Petersburg Academy of Sciences the same year; the construction is based on the observation that the product of two sums of four squares can itself be expressed as a sum of four squares. This idea was used in 1754 by Euler to make partial progress, which led Lagrange, in the same year as the letter, to the first complete proof of the *four square theorem*: every positive integer is the sum of at most four squares [5, 19].

68^2	29^2	41^2	37^2
17^2	31^2	79^2	32^2
59^2	28^2	23^2	61^2
11^2	77^2	8^2	49^2

Fig. 1 Euler's 4×4 magic square of squares with magic constant 8515

The search for a 3×3 magic square of squares was popularized by Martin Gardner in 1996 offering a \$100 prize to the first person to construct such a square, though the problem had already been posed by Edouard Lucas in 1876 and Martin LaBar in 1984 [5, 19]. Despite the great interest and efforts, the prize remains unclaimed (as do the €1000 and bottle of champagne offered by Boyer [4] for the same problem). However, there are a number of results making progress on this problem, for which a comprehensive list can be found in [4]. A 3×3 magic square of squares gives rise to a rational point with nonzero coordinates on a surface cut out by 6 quadrics in the space $\mathbb{P}^8$. A deep conjecture of Lang predicts that this surface contains only finitely many curves of genus 0 or 1, and that outside of these curves it has only finitely many rational points. The method of [6] establishes that indeed this surface contains only finitely many curves of genus 0 or 1. In fact, we know the surface contains curves of genus 0 or 1 which do not correspond to magic squares (for instance, lines parametrisising repeated entries). Therefore, it seems plausible that perhaps there are no 3×3 magic squares of squares, or that they are remarkably rare.

An $n \times n$ magic square of squares corresponds to a rational point on a variety cut out by $2n$ quadrics in the space $\mathbb{P}^{n^2-1}$. In contrast to the $n = 3$ case, it is quite reasonable from a geometric point of view that these spaces would carry many rational points for $n \geq 5$ [19]. This line of logic has led Várilly-Alvarado to make the following conjecture.

Conjecture 1.1 ([19, Conjecture 4.3]) *There is a positive integer $n_0(2)$ such that for every integer $n \geq n_0(2)$, there exists an $n \times n$ magic square of squares.*

In the light of Euler's example above, Várilly-Alvarado further suggested that the conjecture holds with $n_0(2) = 4$. We establish that this is indeed the case.

Theorem 1.2 *For every integer $n \geq 4$, there exists an $n \times n$ magic square of squares.*

In fact, we also establish a generalisation of the conjecture for higher powers.

Theorem 1.3 *Let $d \geq 3$. There is a positive integer $n_0(d)$ such that for every integer $n \geq n_0(d)$, there exists an $n \times n$ magic square of d^{th} powers.*

The novel feature of our work, in comparison to prior work on magic squares in the literature, is that we are applying the Hardy-Littlewood circle method to a problem, for which all previous results had been based on constructive methods (see Remark 1.4 regarding the independent work by Flores [11]). In particular, our result is non-constructive. We believe this is the first¹ instance, in the literature, of the circle method being applied to study magic squares. Prior to our result, the existence of $n \times n$ magic squares of d^{th} powers was only known for sparse values of n when $d \geq 4$ (for $n = q^d$ with $q \geq 2$ and additionally

¹Here we only mean in terms of magic squares with our definition. In a broader sense, as explained in Remark 1.4, it is second to Flores' paper which appeared on the arXiv on 12/6/2024 while our original version on 13/6/2024.

for small values of n when $4 \leq d \leq 7$), and the existence was also known for n in certain congruence classes when $d \in \{2, 3\}$, while we establish the result for all $n \geq n_0(d)$. We present a more detailed account of the progress on this topic in Section 1.1.

As it can be seen from the proof, the statement of Theorem 1.3 in fact holds with

$$n_0(d) = \begin{cases} 4 \min\{2^d, d(d+1)\} + 20 & \text{if } 3 \leq d \leq 4, \\ 4\lceil d(\log d + 4.20032) \rceil + 20 & \text{if } d \geq 5. \end{cases} \quad (1.1)$$

It is worth mentioning that the smallest known example of magic squares of d^{th} powers was of size 2^d for $d \geq 8$; therefore, we improve on the smallest size of magic squares of d^{th} powers known to exist from 2^d to $n_0(d)$ as in (1.1) for $d \geq 9$.

The main challenge in applying the circle method to the equations defining magic squares is that they define a variety which is “too singular” for the method to be directly applicable; this is explained in Section 1.2. Though we can not apply the results for systems of general homogeneous forms by Birch [3] and Rydin Myerson [16], we can apply the version available for systems of diagonal forms by Brüdern and Cook [1]. However, this result requires certain “partitionability” of the coefficient matrix, which amounts to finding a sufficient number of disjoint linearly independent subsets of the columns of the coefficient matrix; establishing this is the main technical challenge of the paper. We prove an optimal (up to a constant) lower bound for this quantity in Theorem 2.4. In this context, the circle method allow us to transform the problem of considerable complexity of finding magic squares of d^{th} powers to a theoretically and computationally simpler problem of finding disjoint linearly independent subsets of the columns of the coefficient matrix. We expect that this lower bound will be particularly useful for studying other variants of magic squares. We believe that our Theorems 1.2 and 1.3 are a significant step towards the complete classification of the existence of $n \times n$ magic squares of d^{th} powers.

1.1 Progress on magic squares of powers

An $n \times n$ magic square is a d -multimagic square if it remains a magic square when all the entries are raised to the i^{th} power for every $i = 2, \dots, d$. It is called a normal d -multimagic square if it is a d -multimagic square with entries consisting of the numbers 1 up to n^2 . Clearly a normal d -multimagic square provides an example of a magic square of d^{th} powers. The first published 2-multimagic squares, which were of sizes 8×8 and 9×9 , were obtained by Pfeffermann in 1890. The first 3-multimagic square was obtained in 1905 by Tarry. In fact, Tarry was the first to devise a systematic method of constructing 2-multimagic and 3-multimagic squares [14]. Prior to our Theorem 1.3, all known examples of magic squares of d^{th} powers for $d \geq 8$ in fact came from multimagic squares. For 2-multimagic squares it was proved by Chen, Li, Pan and Xu [15] that there exists a $2m \times 2m$ normal 2-multimagic squares for all $m \geq 4$. There is also a result by Hu, Meng, Pan, Su and Xiong [12] which establishes the existence of $16m \times 16m$ normal 3-multimagic squares for all $m \geq 1$. We refer the reader to the introductions of [15], [12] and [13] for more detailed history on the progress regarding normal 2 and 3-multimagic squares. The most general result regarding multimagic squares is given by Derksen, Eggermont and van der Essen [9] who have proved that there exist $n \times n$ normal d -multimagic squares for any $n = q^d$ with $q \geq 2$. There is also a comprehensive list of various magic squares recorded by Boyer [4] which includes the following:

- $n \times n$ magic squares of squares for $4 \leq n \leq 7$.
- $n \times n$ 2-multimagic squares for $8 \leq n \leq 64$.
- number of magic squares of d^{th} powers for $2 \leq d \leq 7$.

Thus we see that our Theorems 1.2 and 1.3 are the first result of this type and of different nature compared to all the previous results on magic squares in the literature.

Remark 1.4 It is important to mention the very nice work by Flores [11] here. It was completely unknown to us that he was simultaneously working on an adjacent problem until his preprint appeared on the arXiv on 12/6/2024 which prompted us to post our original version on 13/6/2024. Flores established the existence of $n \times n$ “non-trivial” d -multimagic squares for all $n \geq 2d(d+1)+1$ also using the circle method. Strictly speaking, however, his non-trivial multimagic square is not a magic square in the sense of Conjecture 1.1, because it allows repeated entries; this is an important distinction for us, because for example 3×3 magic squares of squares with repeated entries are known to exist while the big open problem is regarding the existence of one without. Though it is not dealt with in his paper, there is no doubt that Flores’ work can be adapted to deal with multimagic squares without repeated entries as well.

1.2 Application of the Hardy-Littlewood circle method

Let us label the entries of the $n \times n$ magic square of d^{th} powers as follows:

$$\begin{array}{|c|c|c|} \hline x_{1,1}^d & \cdots & x_{1,n}^d \\ \hline \vdots & \vdots & \vdots \\ \hline x_{n,1}^d & \cdots & x_{n,n}^d \\ \hline \end{array}.$$

Let μ be a positive integer. The system of equations defining the $n \times n$ magic square of d^{th} powers with magic constant μ is equivalent to

$$\begin{aligned} x_{1,1}^d + \cdots + x_{1,n}^d &= \mu \\ &\vdots \\ x_{n,1}^d + \cdots + x_{n,n}^d &= \mu \\ x_{1,1}^d + \cdots + x_{n,1}^d &= \mu \\ &\vdots \\ x_{1,n-1}^d + \cdots + x_{n,n-1}^d &= \mu \\ x_{1,1}^d + \cdots + x_{n,n}^d &= \mu \\ x_{1,n}^d + \cdots + x_{n,1}^d &= \mu, \end{aligned} \tag{1.2}$$

which we denote by $F_0(\mathbf{x}_0) = \mu$. A priori the system of equations defining the $n \times n$ magic square of d^{th} powers with magic constant μ requires $2n + 2$ equations; however, it can be verified that there is one degree of redundancy (the $2n - 1$ equations corresponding to n rows and $n - 1$ columns imply the equation corresponding to the remaining column²).

² The assertion that $x_{i,1}^d + \cdots + x_{i,n}^d = \mu$ ($1 \leq i \leq n$) and $x_{1,j}^d + \cdots + x_{n,j}^d = \mu$ ($1 \leq j \leq n-1$) imply $x_{1,n}^d + \cdots + x_{n,n}^d = \mu$ follows from the identity

$$\sum_{i=1}^n x_{i,1}^d + \cdots + x_{i,n}^d = \sum_{j=1}^n x_{1,j}^d + \cdots + x_{n,j}^d.$$

Therefore, this is a system of equations defined by $R_0 = 2n + 1$ degree d homogeneous polynomials in $N_0 = n^2$ variables. Since the number of variables N_0 grows quadratically with R_0 , it may seem reasonable at first to expect that the known results regarding the Hardy-Littlewood circle method readily apply to this system. As it turns out, the system (1.2) is “too singular” for this to be the case.

A seminal result by Birch [3] establishes the existence of a non-trivial integral solution to a general system of equations $F_1(\mathbf{x}) = \cdots = F_R(\mathbf{x}) = 0$ defined by R homogeneous polynomials of degree d in N variables. For $d = 2$, this was greatly improved by Rydin Myerson [16]. An important quantity in these results is the dimension of the singular locus of the pencil

$$\sigma_{\mathbb{R}}(\mathbf{F}) = \max_{\beta \in \mathbb{R}^R} \dim\{\mathbf{x} \in \mathbb{A}^N : \beta \cdot \nabla \mathbf{F}(\mathbf{x}) = \mathbf{0}\},$$

where $\mathbf{F} = (F_1, \dots, F_R)$. The required bound for $\sigma_{\mathbb{R}}(\mathbf{F})$ is $N > \sigma_{\mathbb{R}}(\mathbf{F}) + (d-1)2^{d-1}R(R+1)$ for Birch’s result to be applicable, while $N > \sigma_{\mathbb{R}}(\mathbf{F}) + 8R$ for Rydin Myerson’s result. However, it can be verified that

$$\sigma_{\mathbb{R}}(\mathbf{F}_0) \geq n^2 - n = N_0 - \frac{R_0 - 1}{2},$$

which is far too large to make use of either of the mentioned results. Both of these results are for general systems of homogeneous polynomials; however, the system (1.2) consists only of diagonal polynomials and there are results in this direction as well. Let us now suppose that $F_1, \dots, F_R$ are diagonal polynomials. The system of diagonal equations $F_1(\mathbf{x}) = \cdots = F_R(\mathbf{x}) = 0$ was first studied by Davenport and Lewis [10, Lemma 32]; their result required

$$N \geq \begin{cases} \lfloor 9R^2d \log(3Rd) \rfloor & \text{if } d \text{ is odd,} \\ \lfloor 48R^2d^3 \log(3Rd^2) \rfloor & \text{if } d \geq 4 \text{ is even,} \end{cases}$$

to establish the existence of a non-trivial integral solution. Since $N_0 = (R_0 - 1)^2/4$, we can not hope to directly apply this result to (1.2). By incorporating the breakthrough on Waring’s problem by Vaughan [20], Brüdern and Cook [1] improved the number of variables required to be

$$N \geq 2dR(\log d + O(\log \log d)).$$

We remark that both of these results require a suitable “rank condition” on the coefficient matrix. Since the time of these two papers, there has been great progress regarding Waring’s problem (for example, by Wooley [21], [22] and more recently by Wooley and Brüdern [7]) and also the resolution of Vinogradov’s mean value theorem (see the work by Bourgain, Demeter and Guth [2], and by Wooley [23, 24]). By incorporating these recent developments, the required number of variables may be further improved. Though this technical procedure is mostly standard, we present the details in our separate paper [17] and the result applied to the system (1.2) is summarised in Theorem 2.2.

Notation

We make use of the standard abbreviations $e(z) = e^{2\pi iz}$ and $e_q(z) = e^{\frac{2\pi iz}{q}}$. Given a vector $\mathbf{a} = (a_1, \dots, a_R) \in \mathbb{Z}^R$, by $1 \leq \mathbf{a} \leq q$ we mean $1 \leq a_i \leq q$ for each $1 \leq i \leq R$.

2 Magic squares of powers

Let μ be a positive integer. Let M_0 be the coefficient matrix of the system (1.2), which is given by (5.1). We define

$$\mathcal{J} = \{0\} \cup \{(i_1, j_1; i_2, j_2) : (i_1, j_1) \neq (i_2, j_2), 1 \leq i_1, j_1, i_2, j_2 \leq n\}.$$

For each $\sigma = (i_1, j_1; i_2, j_2) \in \mathcal{J} \setminus \{0\}$, we denote $\mathbf{x}_\sigma$ to be $\mathbf{x}_0$ with x_{i_2, j_2} removed and $\mathbf{F}_\sigma(\mathbf{x}_\sigma) = \mu$ the system of equations obtained by substituting $x_{i_2, j_2} = x_{i_1, j_1}$ into $\mathbf{F}_0(\mathbf{x}_0) = \mu$. We then denote by M_σ the coefficient matrix of this system, which is obtained from M_0 by adding the $((i_2 - 1)n + j_2)$ -th column to the $((i_1 - 1)n + j_1)$ -th column and then deleting the $((i_2 - 1)n + j_2)$ -th column (here $((i - 1)n + j)$ -th column corresponds to the x_{ij} variable).

For $\sigma \in \mathcal{J}$, $\mathfrak{B} \subseteq \mathbb{N}$ and $X \geq 1$, we introduce the following counting function

$$N_\sigma(\mathfrak{B}; X, \mu) = \#\{\mathbf{x}_\sigma \in (\mathfrak{B} \cap [1, X])^{n^2 - \epsilon(\sigma)} : \mathbf{F}_\sigma(\mathbf{x}_\sigma) = \mu\},$$

where

$$\epsilon(\sigma) = \begin{cases} 0 & \text{if } \sigma = 0, \\ 1 & \text{if } \sigma \in \mathcal{J} \setminus \{0\}. \end{cases}$$

Then the number of magic squares, whose entries are restricted to $\mathfrak{B}$, with magic constant μ is given by

$$N(\mathfrak{B}; X, \mu) = N_0(\mathfrak{B}; X, \mu) + O\left(\sum_{\sigma \in \mathcal{J} \setminus \{0\}} N_\sigma(\mathfrak{B}; X, \mu)\right). \quad (2.1)$$

In this expression, the sum in the O -term is the contribution from squares whose entries are not distinct. We estimate these counting functions using the Hardy-Littlewood circle method for $\mathfrak{B} = \mathbb{N}$ and

$$\mathcal{A}(X, X^\eta) = \{x \in [1, X] \cap \mathbb{N} : \text{prime } p|x \text{ implies } p \leq X^\eta\}$$

for sufficiently small $\eta > 0$. The optimal lower bound for $n_0(d)$ in Theorem 1.3 will come from using smooth numbers for most choices of d , while for $d \in \{2, 3, 4\}$ it will come from the natural numbers instead.

Definition 2.1 Let $\sigma \in \mathcal{J}$. We define $\Psi(M_\sigma)$ to be the largest integer T such that there exists

$$\{\mathfrak{D}_1, \dots, \mathfrak{D}_T\},$$

where each $\mathfrak{D}_i$ is a linearly independent set of $2n + 1$ columns of M_σ and $\mathfrak{D}_i \cap \mathfrak{D}_j \neq \emptyset$ if $i \neq j$. We let T_σ be a non-negative integer such that

$$\Psi(M_\sigma) \geq T_\sigma.$$

By applying the circle method to the system of diagonal equations (1.2), we obtain the following as a direct consequence of [17, Theorems 1.4 and 1.5]. Here, we present a simplified version of the result (see [17, Tables 1 and 2] for more accurate values and also [17, Remark 2.3]).

Theorem 2.2 *Let $\mathfrak{B} = \mathbb{N}$ or $\mathcal{A}(X, X^\eta)$ with $\eta > 0$ sufficiently small. Suppose*

$$\min_{\sigma \in \mathcal{J}} T_\sigma \geq \begin{cases} \min\{2^d, d(d+1)\} + 1 & \text{if } 2 \leq d \leq 4 \text{ and } \mathfrak{B} = \mathbb{N}, \\ \lceil d(\log d + 4.20032) \rceil + 1 & \text{if } d \geq 5 \text{ and } \mathfrak{B} = \mathcal{A}(X, X^\eta). \end{cases}$$

Then there exists $\lambda > 0$ such that

$$N_0(\mathfrak{B}; X, \mu) = C_{\mathfrak{B}} \mathfrak{S} \mathfrak{I} X^{n^2 - (2n+1)d} + O(X^{n^2 - (2n+1)d} (\log X)^{-\lambda}),$$

where

$$C_{\mathfrak{B}} = \begin{cases} 1 & \text{if } \mathfrak{B} = \mathbb{N}, \\ c(\eta) & \text{if } \mathfrak{B} = \mathcal{A}(X, X^\eta), \end{cases}$$

$c(\eta) > 0$ is a constant depending only on η , the singular series $\mathfrak{S}$ and the singular integral $\mathfrak{I}$ are defined in (3.1) and (3.3), respectively. Furthermore,

$$\max_{\sigma \in \mathcal{J} \setminus \{0\}} N_\sigma(\mathfrak{B}; X, \mu) \ll X^{n^2 - (2n+1)d - 1}.$$

The next step is to establish lower bounds for $\mathfrak{S}$ and $\mathfrak{I}$ which are independent of X . We present the details of the following proposition in Section 3.

Proposition 2.3 *Given any $X \geq 1$ sufficiently large, there exists $\mu = \mu(X) \in \mathbb{N}$ such that*

$$\mathfrak{S} \mathfrak{I} > c_{n,d}$$

where $c_{n,d} > 0$ is a constant depending only on n and d .

Finally, in order to establish the existence of magic squares of d^{th} powers with magic constant μ , it remains to establish a lower bound for T_σ . The following is the main technical result of the paper, which we prove through Sections 4–6.

Theorem 2.4 *Let $n \geq 8$. Then*

$$T_0 \geq \left\lfloor \frac{n}{4} \right\rfloor - 1.$$

We suspect that the constant 4 appearing in the denominator of this inequality is not optimal. By combining these results collected in this section, we obtain Theorem 1.3 as an immediate consequence.

Proof of Theorem 1.3 It follows from Theorem 2.4 that

$$\min_{\sigma \in \mathcal{J} \setminus \{0\}} T_\sigma \geq T_0 - 2 \geq \left\lfloor \frac{n}{4} \right\rfloor - 3.$$

Therefore, by combining this estimate, Theorem 2.2 and Proposition 2.3 with (2.1), we obtain that Theorem 1.3 holds with

$$n_0(d) = \begin{cases} 4 \min\{2^d, d(d+1)\} + 20 & \text{if } 2 \leq d \leq 4, \\ 4 \lceil d(\log d + 4.20032) \rceil + 20 & \text{if } d \geq 5. \end{cases} \quad (2.2)$$

□

In order to establish Theorem 1.2 we need to deal with smaller values of n .

Proof of Theorem 1.2 It follows from the proof of Theorem 1.3 above that there exists an $n \times n$ magic square of squares as soon as $n \geq 36$. Since the statement is already known for $4 \leq n \leq 64$, in fact explicit examples have been discovered and listed in [4], this completes the proof. $\square$

3 Singular series and singular integral: Proof of Proposition 2.3

We let $\text{Col}(M_0)$ denote the set of columns of M_0 . Let Jac_{F_0} denote the Jacobian matrix of F_0 and $\mathbb{F} = \mathbb{R}$ or $\mathbb{Q}_p$ for any prime p . A crucial fact we make use of in this section is that given any $z \in \mathbb{F} \setminus \{0\}$, we have

$$\text{Jac}_{F_0}(z, \dots, z) = dz^{d-1}M_0,$$

which in particular is of full rank. Therefore, if $F_0(z, \dots, z) = \mu$, then it is in fact a non-singular solution.

Let

$$S(q, a) = \sum_{1 \leq x \leq q} e_q(ax^d).$$

We define the singular series

$$\mathfrak{S} = \sum_{q=1}^{\infty} A(q), \quad (3.1)$$

where

$$A(q) = q^{-n^2} \sum_{\substack{1 \leq \mathbf{a} \leq q \\ \gcd(q, \mathbf{a})=1}} \prod_{\mathbf{c} \in \text{Col}(M_0)} S(q, \mathbf{a} \cdot \mathbf{c}) \cdot e_q \left(-\mu \sum_{i=1}^{2n+1} a_i \right).$$

We have the following lemma regarding $\mathfrak{S}$ which is [17, Lemmas 4.1 and 4.2].

Lemma 3.1 Suppose $T_0 > 2d$. Then

$$A(q) \ll q^{-\frac{T_0}{d} + 1 + \varepsilon}, \quad (3.2)$$

for any $\varepsilon > 0$ sufficiently small, where the implicit constant is independent of μ , and the series (3.1) converges absolutely. In fact,

$$\mathfrak{S} = \prod_{p \text{ prime}} \chi(p),$$

where

$$\chi(p) = 1 + \sum_{k=1}^{\infty} A(p^k).$$

We establish the desired lower bound for $\mathfrak{S}$ for special values of μ .

Lemma 3.2 Let $\mu = np_0^d$, where p_0 is a prime number sufficiently large with respect to n and d . Then $\mathfrak{S} > c_{n,d}$, where $c_{n,d} > 0$ is a constant depending only on n and d .

Proof An application of (3.2) yields

$$|\chi(p) - 1| \ll \sum_{k=1}^{\infty} p^{k(-\frac{T_0}{d} + 1 + \varepsilon)} \ll p^{-\frac{T_0}{d} + 1 + \varepsilon}.$$

Therefore, there exists $P > 0$ such that

$$\prod_{p > P} \chi(p) > \frac{1}{2}.$$

We remark that P is independent of μ . The standard argument shows that

$$\chi(p) = \lim_{m \rightarrow \infty} \frac{v_{\mu}(p^m)}{p^{m(n^2 - 2n - 1)}},$$

where $v_{\mu}(p^m)$ is the number of solutions to the congruence $\mathbf{F}_0(\mathbf{x}_0) \equiv \mu \pmod{p^m}$. Since $\mu = np_0^d$ with prime p_0 sufficiently large and p_0 is invertible modulo p for $p \leq P$, it follows that

$$v_{\mu}(p^m) = v_n(p^m).$$

We know that $\mathbf{x}_0 = (1, \dots, 1) \in \mathbb{Z}_p^{n^2}$ is a non-singular solution to the system of equations $\mathbf{F}_0(\mathbf{x}_0) = \mathbf{n}$. Thus it follows from Hensel's lemma that

$$\chi(p) = \lim_{m \rightarrow \infty} \frac{v_{\mu}(p^m)}{p^{m(n^2 - 2n - 1)}} = \lim_{m \rightarrow \infty} \frac{\lambda_n(p^m)}{p^{m(n^2 - 2n - 1)}} > 0$$

for $p \leq P$. Therefore, we obtain

$$\mathfrak{S} > \frac{1}{2} \prod_{p \leq P} \chi(p) \gg 1,$$

where the implicit constant is independent of μ . □

Let

$$I(\beta) = \int_0^1 e(\beta \xi^d) d\xi.$$

We define the singular integral

$$\mathfrak{I} = \int_{\mathbb{R}^{2n+1}} \prod_{\mathbf{c} \in \text{Col}(M_0)} I(\gamma \cdot \mathbf{c}) \cdot e\left(-\frac{\mu}{X^d} \sum_{i=1}^{2n+1} \gamma_i\right) d\gamma. \quad (3.3)$$

We have the following lemma regarding $\mathfrak{I}$ which is [17, Lemmas 4.3]

Lemma 3.3 *Suppose $T_0 > d$. Then the integral (3.3) converges absolutely.*

We establish the desired lower bound for $\mathfrak{I}$ for special values of μ .

Lemma 3.4 *Let $\varepsilon_0 > 0$ be sufficiently small. Suppose $\mu = n\zeta^d X^d$ with $\zeta \in [\varepsilon_0, 1 - \varepsilon_0]$. Then $\mathfrak{I} > c_{n,d,\varepsilon_0}$, where $c_{n,d,\varepsilon_0} > 0$ is a constant depending only on n, d and ε_0 .*

Proof It follows by the standard argument as in [18] that

$$\mathfrak{I} = \lim_{L \rightarrow \infty} \int_{[0,1]^{n^2}} \prod_{i=1}^{2n+1} \Phi_L(F_{0,i}(\mathbf{x}_0) - \mu X^{-d}) d\mathbf{x}_0,$$

where

$$\Phi_L(\eta) = \begin{cases} L(1 - L|\eta|) & \text{if } |\eta| \leq L^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, since $\mu X^{-d} = n\zeta^d$ with $\zeta \in [\varepsilon_0, 1 - \varepsilon_0]$, we see that $\mathbf{x}_0 = (\zeta, \dots, \zeta)$ is a non-singular solution to the system of equations $\mathbf{F}_0(\mathbf{x}_0) = \mu$. It then follows by an application of the implicit function theorem as in [18, Lemma 2] that $\mathfrak{I} > 0$. In particular, since $\zeta \in [\varepsilon_0, 1 - \varepsilon_0]$, the lower bound is independent of μ . $\square$

Let $\varepsilon_0 > 0$ be sufficiently small. By the prime number theorem, for any X sufficiently large there exists a prime p_0 satisfying

$$\varepsilon_0 X < p_0 < (1 - \varepsilon_0)X.$$

Then for $\mu = np_0^d$ we see that Lemmas 3.2 and 3.4 hold, from which Proposition 2.3 follows.

4 Linear equations

In this section, we record a simple result regarding certain systems of linear equations which we will need in the following Section 6.1. Let $1 \leq i_1 < m < m+1 < i_2 \leq n$. We denote by $\mathbb{L}_n(i_1; m; i_2)$ the system of $2n$ linear equations

$$\begin{aligned} x_i + y_i &= 0 \quad (1 \leq i \leq n) \\ x_{i+1} + y_i &= 0 \quad (i \neq i_1 - 1, i_1, i_2 - 1, i_2, m) \\ x_{i_2} + y_{i_1-1} &= 0 \\ x_{i_2+1} + y_{i_1} &= 0 \\ x_{i_1} + y_{i_2-1} &= 0 \\ x_{i_1+1} + y_{i_2} &= 0 \\ y_m &= 0, \end{aligned}$$

where x_{n+1} is identified as x_1 .

Lemma 4.1 Suppose $1 < i_1 < m < m+1 < i_2 < n$. Then

$$\{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{2n} : (\mathbf{x}, \mathbf{y}) \text{ satisfies } \mathbb{L}_n(i_1; m; i_2)\} = \{\mathbf{0}\}.$$

Proof Consider the system of equations $\mathbb{L}_n(i_1; m; i_2)$. By substituting $y_m = 0$ into the equation $x_m + y_m = 0$ and following through with the consequences, we obtain

$$x_i = y_i = 0 \quad (i \in [i_1 + 1, m]).$$

We can then deduce that

$$0 = x_{i_1+1} = y_{i_2} = x_{i_2} = y_{i_1-1} = x_{i_1-1},$$

which further implies that

$$x_i = y_i = 0 \quad (i \in [1, i_1 - 1]).$$

Therefore, the system becomes

$$\begin{aligned} x_{i_1} + y_{i_1} &= 0 & x_{i_2+1} + y_{i_1} &= 0 \\ x_{m+1} + y_{m+1} &= 0 & x_{m+2} + y_{m+1} &= 0 \\ &\vdots \\ x_{i_2-2} + y_{i_2-2} &= 0 & x_{i_2-1} + y_{i_2-2} &= 0 \\ x_{i_2-1} + y_{i_2-1} &= 0 & x_{i_1} + y_{i_2-1} &= 0 \\ x_i + y_i &= 0 & x_{i+1} + y_i &= 0 \quad (i \in [i_2 + 1, n]). \end{aligned}$$

By substituting $x_1 = 0$, we obtain

$$x_i = y_i = 0 \quad (i \in [i_2 + 1, n]).$$

which further implies that

$$0 = x_{i_2+1} = y_{i_1} = x_{i_1} = y_{i_2-1}.$$

Finally, by substituting $y_{i_2-1} = 0$ into the remaining system, we see that

$$x_i = y_i = 0 \quad (i \in [m + 1, i_2 - 1])$$

as desired. $\square$

5 Preliminaries

Let I_n denote the $n \times n$ identity matrix and define $\tilde{I}_n$ to be the $(n - 1) \times n$ matrix obtained by removing the last row from I_n . Then the $(2n + 1) \times n^2$ coefficient matrix of the system (1.2) is

$$M_0 = \begin{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} & \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} & \cdots & \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix} \\ \tilde{I}_n & \tilde{I}_n & \cdots & \tilde{I}_n \\ \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} & \cdots & \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix} \end{bmatrix}. \quad (5.1)$$

We shall denote by $\mathbf{c}_{i,j}$ the $((i - 1)n + j)$ -th column of M_0 , for each $1 \leq i, j \leq n$. The first subscript i will always satisfy $1 \leq i \leq n$, but for the second subscript j , to simplify our exposition, we will consider it modulo n , that is

$$c_{i,j+mn} = c_{i,j},$$

for any $1 \leq j \leq n$ and $m \in \mathbb{Z}$.

Definition 5.1 We shall refer to the set $\{\mathbf{c}_{i,1}, \dots, \mathbf{c}_{i,n}\}$ as the i -th block for each $1 \leq i \leq n$.

Given $\mathfrak{B} \subseteq \text{Col}(M_0)$, we define

$$\mathfrak{B}[i] = \{1 \leq j \leq n : \mathbf{c}_{ij} \in \mathfrak{B}\} \quad (5.2)$$

for each $1 \leq i \leq n$.

Let

$$\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2,$$

where

$$\mathcal{S}_1 = \{\mathbf{c}_{1,1}, \mathbf{c}_{2,2}, \dots, \mathbf{c}_{n-1,n-1}, \mathbf{c}_{n,n}\}$$

and

$$\mathcal{S}_2 = \{\mathbf{c}_{1,n}, \mathbf{c}_{2,n-1}, \dots, \mathbf{c}_{n-1,2}, \mathbf{c}_{n,1}\} \setminus \mathcal{S}_1.$$

The columns in $\mathcal{S}_1$ are precisely the ones with 1 in the $2n$ -th entry and $\mathcal{S}_2$ the ones with 1 in the $(2n+1)$ -th entry that are not contained in $\mathcal{S}_1$. We remark that

$$\#\mathcal{S}_2 = \begin{cases} n & \text{if } n \text{ is even,} \\ n-1 & \text{if } n \text{ is odd.} \end{cases}$$

Let us define

$$\epsilon(n) = \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd,} \end{cases} \quad (5.3)$$

and

$$N = \frac{n-1+\epsilon(n)}{2} - 2. \quad (5.4)$$

For each $0 \leq \ell \leq N$, we define

$$\tilde{\mathfrak{B}}_\ell = \{\mathbf{c}_{1,1+2\ell}, \mathbf{c}_{2,2+2\ell}, \dots, \mathbf{c}_{n,n+2\ell}\} \cup (\{\mathbf{c}_{1,1+(2\ell+1)}, \mathbf{c}_{2,2+(2\ell+1)}, \dots, \mathbf{c}_{n,n+(2\ell+1)}\} \setminus \{\mathbf{c}_{n-2\ell-1,n}\}).$$

This set contains precisely one column of the form $\mathbf{c}_{*,n}$, which is $\mathbf{c}_{n-2\ell,n}$, a column whose entries between $(n+1)$ -th and $(2n-1)$ -th position are all 0. We will use these sets $\tilde{\mathfrak{B}}_\ell$ to construct the collection of pairwise disjoint sets of $2n+1$ linearly independent columns of M necessary to complete the proof of Theorem 2.4.

By (5.4) it follows that

$$\tilde{\mathfrak{B}}_\ell \cap \tilde{\mathfrak{B}}_{\ell'} = \emptyset \quad (0 \leq \ell < \ell' \leq N). \quad (5.5)$$

Lemma 5.2 *Given any $1 \leq \ell \leq N$, we have*

$$\tilde{\mathfrak{B}}_\ell \cap \mathcal{S} = \left\{ \mathbf{c}_{\frac{n+1-\epsilon(n)}{2}-\ell, \frac{n+1-\epsilon(n)}{2}+\epsilon(n)+\ell}, \mathbf{c}_{n-\ell, \ell+1} \right\}.$$

Proof Since $\mathcal{S}_1 \subseteq \tilde{\mathfrak{B}}_0$, it follows from (5.5) that

$$\tilde{\mathfrak{B}}_\ell \cap \mathcal{S}_1 = \emptyset.$$

Therefore, if $\tilde{\mathfrak{B}}_\ell \cap \mathcal{S} \neq \emptyset$, then there exist $\epsilon \in \{0, 1\}$ and $1 \leq i, j \leq n$ such that

$$(i, i+2\ell+\epsilon+m(i, \ell, \epsilon)n) = (j, n+1-j),$$

where

$$m(i, \ell, \epsilon) = \begin{cases} 0 & \text{if } 1 \leq i + 2\ell + \epsilon \leq n, \\ -1 & \text{if } n < i + 2\ell + \epsilon \leq 2n. \end{cases}$$

It follows that $i = j$ and

$$j + 2\ell + \epsilon + m(j, \ell, \epsilon)n = n + 1 - j,$$

or equivalently

$$j = \frac{n + 1 - \epsilon}{2} - \ell - \frac{m(j, \ell, \epsilon)n}{2}.$$

Suppose $m(j, \ell, \epsilon) = 0$. Then it must be that $\epsilon = 1$ if n is even and 0 if n is odd. Thus we see that

$$\mathbf{c}_{\frac{n+1-\epsilon(n)}{2}-\ell, \frac{n+1-\epsilon(n)}{2}+\epsilon(n)+\ell} \in \tilde{\mathfrak{B}}_\ell \cap \mathcal{S};$$

here we note that $1 \leq \frac{n+1-\epsilon(n)}{2} + \epsilon(n) + \ell \leq n$.

On the other hand, suppose $m(j, \ell, \epsilon) = -1$. Then

$$j = n + \frac{1 - \epsilon}{2} - \ell.$$

In particular, it must be that $\epsilon = 1$. Thus we see that

$$\mathbf{c}_{n-\ell, \ell+1} \in \tilde{\mathfrak{B}}_\ell \cap \mathcal{S}.$$

Finally, we have $\mathbf{c}_{\frac{n+1-\epsilon(n)}{2}-\ell, \frac{n+1-\epsilon(n)}{2}+\epsilon(n)+\ell} \neq \mathbf{c}_{n-\ell, \ell+1}$, since

$$1 \leq \frac{n + 1 - \epsilon(n)}{2} - \ell \leq \frac{n}{2} - \ell < n - \ell.$$

□

As a consequence of this lemma, there are precisely two columns in $\tilde{\mathfrak{B}}_\ell$ whose last two entries are not 0. In the next section, we replace these two columns from $\tilde{\mathfrak{B}}_\ell$ with appropriate columns whose last two entries are 0 such that the resulting set is linearly independent. Finally, we complete the sets by adding two columns whose last two entries are not 0 which preserve the linear independence.

6 Proof of Theorem 2.4

Let $n \geq 8$ and $1 \leq \ell \leq N$, where N is defined in (5.4). Our goal is to replace the two columns in $\tilde{\mathfrak{B}}_\ell$ from Lemma 5.2 in a suitable manner so that all columns have 0 for the last two entries. Let us denote

$$i_1(\ell) = \frac{n + 1 - \epsilon(n)}{2} - \ell \quad \text{and} \quad i_2(\ell) = n - \ell,$$

where $\epsilon(n)$ is defined in (5.3). Then the two columns we need to replace are

$$\mathbf{c}_{\frac{n+1-\epsilon(n)}{2}-\ell, \frac{n+1-\epsilon(n)}{2}+\epsilon(n)+\ell} = \mathbf{c}_{i_1(\ell), i_1(\ell)+2\ell+\epsilon(n)} \quad \text{and} \quad \mathbf{c}_{n-\ell, \ell+1} = \mathbf{c}_{i_2(\ell), i_2(\ell)+2\ell+1}.$$

We shall modify $\tilde{\mathfrak{B}}_\ell$ as follows

$$\mathfrak{B}_\ell = \tilde{\mathfrak{B}}_\ell \setminus \left(\{\mathbf{c}_{i_1(\ell), i_1(\ell)+2\ell}, \mathbf{c}_{i_1(\ell), i_1(\ell)+2\ell+1}\} \cup \{\mathbf{c}_{i_2(\ell), i_2(\ell)+2\ell}, \mathbf{c}_{i_2(\ell), i_2(\ell)+2\ell+1}\} \right) \\ \cup \{\mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell}, \mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell+1}\} \cup \{\mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell}, \mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell+1}\},$$

that is we first remove the two columns in $\tilde{\mathfrak{B}}_\ell$ from the $i_1(\ell)$ -th and $i_2(\ell)$ -th block and then add back in two columns from each of these blocks with switched positions. We remark that we know there are two columns in $\tilde{\mathfrak{B}}_\ell$ from the $i_1(\ell)$ -th and $i_2(\ell)$ -th block, because

$$1 < i_1(\ell) < n - 2\ell - 1 < n - 2\ell < i_2(\ell) < n. \quad (6.1)$$

It is clear that given $1 \leq \ell < \ell' \leq N$ we have

$$\{i_1(\ell), i_2(\ell)\} \cap \{i_1(\ell'), i_2(\ell')\} = \emptyset. \quad (6.2)$$

Therefore, the two blocks of $\tilde{\mathfrak{B}}_\ell$ which get modified to construct $\mathfrak{B}_\ell$ are unique to ℓ . Let us also recall the notation (5.2) and record the relations

$$\mathfrak{B}_\ell[i_1(\ell)] = \{i_2(\ell) + 2\ell, i_2(\ell) + 2\ell + 1\} \quad \text{and} \quad \mathfrak{B}_\ell[i_2(\ell)] = \{i_1(\ell) + 2\ell, i_1(\ell) + 2\ell + 1\} \quad (6.3)$$

for each $1 \leq \ell \leq N$.

Lemma 6.1 *Given $1 \leq \ell \leq N$ such that*

$$\ell \neq \begin{cases} \lfloor n/4 \rfloor & \text{if } n \text{ is even,} \\ \lfloor n/4 \rfloor, \lfloor n/4 \rfloor + 1 & \text{if } n \text{ is odd,} \end{cases}$$

we have

$$\{\mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell}, \mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell+1}\} \cap \mathcal{S} = \emptyset$$

and

$$\{\mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell}, \mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell+1}\} \cap \mathcal{S} = \emptyset.$$

In particular, every column of $\mathfrak{B}_\ell$ has 0 for the last two entries.

Proof Let $\epsilon \in \{0, 1\}$. Since it can be verified that

$$i_1(\ell) + i_2(\ell) + 2\ell + \epsilon \equiv \frac{n+1-\epsilon(n)}{2} + \epsilon \not\equiv n+1 \pmod{n}$$

and

$$\pm(i_1(\ell) - i_2(\ell)) \equiv \pm \frac{n+1-\epsilon(n)}{2} \not\equiv 2\ell + \epsilon \pmod{n},$$

the result follows. $\square$

Let $\mathcal{Z} \subseteq \{1, \dots, N\}$ be a set with the following property: given any $m, \ell \in \mathcal{Z}$, we have

$$\frac{n+1-\epsilon(n)}{2} \not\equiv 2(m-\ell) + \delta \pmod{n} \quad (6.4)$$

for any $\delta \in \{-1, 0, 1\}$.

Let us define

$$\mathfrak{R} = \bigcup_{\ell \in \mathcal{Z}} \tilde{\mathfrak{B}}_\ell.$$

Lemma 6.2 *Given $\ell \in \mathcal{L}$, we have*

$$\mathfrak{B}_\ell[i_1(\ell)] \cap \mathfrak{R}[i_1(\ell)] = \emptyset$$

and

$$\mathfrak{B}_\ell[i_2(\ell)] \cap \mathfrak{R}[i_2(\ell)] = \emptyset.$$

Proof First we recall the relations (6.3). Let us suppose

$$\{i_2(\ell) + 2\ell, i_2(\ell) + 2\ell + 1\} \cap \mathfrak{R}[i_1(\ell)] \neq \emptyset.$$

Then there exists $m \in \mathcal{L}$ such that

$$i_2(\ell) + 2\ell + \epsilon \equiv i_1(\ell) + 2m + \epsilon' \pmod{n}$$

for some $\epsilon, \epsilon' \in \{0, 1\}$. Since the congruence is equivalent to

$$\frac{n+1-\epsilon(n)}{2} \equiv 2(\ell-m) + \epsilon - \epsilon' \pmod{n},$$

we reach contradiction by the definition of $\mathcal{L}$.

Similarly, let us suppose

$$\{i_1(\ell) + 2\ell, i_1(\ell) + 2\ell + 1\} \cap \mathfrak{R}[i_2(\ell)] \neq \emptyset.$$

Then there exists $m \in \mathcal{L}$ such that

$$i_1(\ell) + 2\ell + \epsilon \equiv i_2(\ell) + 2m + \epsilon' \pmod{n}$$

for some $\epsilon, \epsilon' \in \{0, 1\}$. From this congruence, we may reach contradiction in the same way as above. $\square$

Lemma 6.3 *We have*

$$\mathfrak{B}_\ell \cap \mathfrak{B}_{\ell'} = \emptyset$$

for any distinct $\ell, \ell' \in \mathcal{L}$.

Proof Let $Z = \#\mathcal{L}$ and denote

$$\mathcal{L} = \{\ell_1, \dots, \ell_Z\}.$$

We shall prove by induction that

$$\mathfrak{B}_{\ell_i} \cap (\mathfrak{B}_{\ell_1} \cup \dots \cup \mathfrak{B}_{\ell_{i-1}} \cup \tilde{\mathfrak{B}}_{\ell_{i+1}} \cup \dots \cup \tilde{\mathfrak{B}}_{\ell_Z}) = \emptyset$$

for each $1 \leq i \leq Z$. The base case $i = 1$ follows easily from (5.5) and Lemma 6.2. Let us suppose the statement holds for all values greater than or equal to 1 and less than i , for some $1 < i \leq Z$. Let $i+1 < j \leq Z$. Then it follows from (5.5) and Lemma 6.2 that

$$\mathfrak{B}_{\ell_{i+1}} \cap \tilde{\mathfrak{B}}_{\ell_j} = (\mathfrak{B}_{\ell_{i+1}} \setminus \tilde{\mathfrak{B}}_{\ell_{i+1}}) \cap \tilde{\mathfrak{B}}_{\ell_j} \subseteq (\mathfrak{B}_{\ell_{i+1}} \setminus \tilde{\mathfrak{B}}_{\ell_{i+1}}) \cap \mathfrak{R} = \emptyset.$$

Therefore, it remains to prove

$$\mathfrak{B}_{\ell_{i+1}} \cap (\mathfrak{B}_{\ell_1} \cup \dots \cup \mathfrak{B}_{\ell_i}) = \emptyset.$$

Since it follows from the inductive hypothesis that

$$\tilde{\mathfrak{B}}_{\ell_{i+1}} \cap \mathfrak{B}_{\ell_s} = \emptyset \quad (1 \leq s \leq i),$$

it suffices to prove

$$(\mathfrak{B}_{\ell_{i+1}} \setminus \tilde{\mathfrak{B}}_{\ell_{i+1}}) \cap \mathfrak{B}_{\ell_s} = \emptyset \quad (1 \leq s \leq i),$$

which in turn follows from

$$\mathfrak{B}_{\ell_{i+1}}[i_1(\ell_{i+1})] \cap \mathfrak{B}_{\ell_s}[i_1(\ell_{i+1})] = \emptyset \quad \text{and} \quad \mathfrak{B}_{\ell_{i+1}}[i_2(\ell_{i+1})] \cap \mathfrak{B}_{\ell_s}[i_2(\ell_{i+1})] = \emptyset \quad (6.5)$$

for all $1 \leq s \leq i$. Since the $i_1(\ell_{i+1})$ -th and $i_2(\ell_{i+1})$ -th block of $\tilde{\mathfrak{B}}_{\ell_s}$ do not get modified to construct $\mathfrak{B}_{\ell_s}$, which follows from (6.2), we obtain

$$\mathfrak{B}_{\ell_s}[i_1(\ell_{i+1})] = \tilde{\mathfrak{B}}_{\ell_s}[i_1(\ell_{i+1})] \subseteq \mathfrak{R}[i_1(\ell_{i+1})]$$

and

$$\mathfrak{B}_{\ell_s}[i_2(\ell_{i+1})] = \tilde{\mathfrak{B}}_{\ell_s}[i_2(\ell_{i+1})] \subseteq \mathfrak{R}[i_2(\ell_{i+1})]$$

for all $1 \leq s \leq i$. Therefore, (6.5) and consequently the result follow from Lemma 6.2. $\square$

Finally, we prove that $\mathfrak{B}_\ell$ is a linearly independent set.

Lemma 6.4 *Given $\ell \in \mathcal{Z} \setminus \{\lfloor n/4 \rfloor, \lfloor n/4 \rfloor + 1\}$, we have*

$$\dim \text{Span}_{\mathbb{R}} \mathfrak{B}_\ell = 2n - 1.$$

Proof Suppose we have the following linear combination of columns in $\mathfrak{B}_\ell$:

$$\begin{aligned} \mathbf{0} = & \sum_{\substack{1 \leq i \leq n \\ i \neq i_1(\ell), i_2(\ell)}} (x_i \mathbf{c}_{i,i+2\ell} + y_i \mathbf{c}_{i,i+2\ell+1}) \\ & + x_{i_1(\ell)} \mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell} + y_{i_1(\ell)} \mathbf{c}_{i_1(\ell), i_2(\ell)+2\ell+1} \\ & + x_{i_2(\ell)} \mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell} + y_{i_2(\ell)} \mathbf{c}_{i_2(\ell), i_1(\ell)+2\ell+1}, \end{aligned} \quad (6.6)$$

with $y_{n-2\ell-1} = 0$ (because we have (6.1) and $\mathbf{c}_{n-2\ell-1,n} \notin \mathfrak{B}_\ell$). Our goal is to show $x_i = y_i = 0$ for all $1 \leq i \leq n$. Let us recall that $\mathbf{c}_{n-2\ell,n} \in \mathfrak{B}_\ell$ whose entries between $(n+1)$ -th and $(2n-1)$ -th positions are all 0. Furthermore, this is the only column in $\mathfrak{B}_\ell$ of the form $\mathbf{c}_{*,n}$, which follows from the definition of $\mathfrak{B}_\ell$ and (6.1). By the definition of $\mathbf{c}_{i,j}$, the vector equation (6.6) is equivalent to the following system of linear equations

$$\begin{aligned} x_i + y_i &= 0 \quad (1 \leq i \leq n) \\ x_{i+1} + y_i &= 0 \quad (i \neq i_1(\ell) - 1, i_1(\ell), i_2(\ell) - 1, i_2(\ell), n - 2\ell - 1) \\ x_{i_2(\ell)} + y_{i_1(\ell)-1} &= 0 \\ x_{i_2(\ell)+1} + y_{i_1(\ell)} &= 0 \\ x_{i_1(\ell)} + y_{i_2(\ell)-1} &= 0 \\ x_{i_1(\ell)+1} + y_{i_2(\ell)} &= 0 \\ y_{n-2\ell-1} &= 0. \end{aligned}$$

It is clear that this system of equations is precisely $\mathbb{L}(i_1(\ell); n - 2\ell - 1; i_2(\ell))$. Therefore, the result follows from Lemma 4.1 since we have (6.1). $\square$

6.1 Final bound for T_0

Let us set

$$\mathcal{Z} = \left\{1, \dots, \left\lfloor \frac{n}{4} \right\rfloor - 1\right\}.$$

Then we have

$$|2(m - \ell) + \delta| \leq 2 \left\lfloor \frac{n}{4} \right\rfloor - 3 \leq \frac{n-6}{2}$$

for any $m, \ell \in \mathcal{Z}$ and $\delta \in \{-1, 0, 1\}$, which implies that $\mathcal{Z}$ satisfies (6.4). Since every column in $\mathfrak{B}_\ell$ has 0 for the last two entries, we obtain the following as an immediate consequence.

Corollary 6.5 *Let $\ell \in \mathcal{Z}$ and $(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_1 \times \mathcal{S}_2$. Then $\mathfrak{B}_\ell \cup \{\mathbf{a}, \mathbf{b}\}$ is a linearly independent set.*

Since

$$\#\mathcal{S}_1, \#\mathcal{S}_2 \geq n-1 \geq |\mathcal{Z}| = \left\lfloor \frac{n}{4} \right\rfloor - 1,$$

and $\mathfrak{B}_\ell$ are pairwise disjoint, we easily obtain $\lfloor n/4 \rfloor - 1$ pairwise disjoint sets of the form

$$\mathfrak{D}_\ell = \mathfrak{B}_\ell \cup \{\mathbf{a}_\ell, \mathbf{b}_\ell\},$$

where $(\mathbf{a}_\ell, \mathbf{b}_\ell) \in \mathcal{S}_1 \times \mathcal{S}_2$. Thus we have established

$$T_0 \geq \left\lfloor \frac{n}{4} \right\rfloor - 1,$$

where T_0 is from the statement of the theorem.

Acknowledgements

The authors are grateful to Tim Browning for his constant encouragement and enthusiasm, Jörg Brüdern for very helpful discussion regarding his paper [1] and Diyan Wu for turning the proof of Theorem 2.4 in the original version into an algorithm and running the computation for us, for which the results are available in the appendix of the original version. They would also like to thank Christian Boyer for maintaining his website [4] which contains a comprehensive list of various magic squares discovered, Brady Haran and Tony Várilly-Alvarado for their public engagement activity of mathematics and magic squares of squares³, and all the magic squares enthusiasts who have contributed to [4] which made this paper possible. Finally, the authors would like to thank the anonymous referees for their helpful comments, Daniel Flores for his work [11] which inspired them to optimise the proof of Theorem 2.4 and Trevor Wooley for very helpful discussion regarding recent developments in Waring's problem and his comments on the original version of this paper.

Funding Open access funding provided by Institute of Science and Technology (IST Austria). NR was supported by FWF project ESP 441-NBL while SY by a FWF grant (DOI 10.55776/P32428).

Data availability The authors declare that the manuscript has no associated data.

Author details

TU Graz, Institute of Analysis and Number Theory, Kopernikusgasse 24/II 8010 Graz, Austria, IST Austria, Am Campus 1, 3400 Klosterneuburg, Austria.

Received: 20 March 2025 Accepted: 3 September 2025

Published online: 23 September 2025

³A YouTube video "Magic Squares of Squares (are PROBABLY impossible)" of the Numberphile channel by Brady Haran, in which Tony Várilly-Alvarado appears as a guest speaker: <https://www.youtube.com/watch?v=Kdsj84UdeYg>.

References

- Brüdern, J., Cook, R.J.: On simultaneous diagonal equations and inequalities. *Acta Arith.* **62**(2), 125–149 (1992)
- Bourgain, J., Demeter, C., Guth, L.: Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math. (2)* **184**(2), 633–682 (2016)
- Birch, B.J.: Forms in many variables. *Proc. Roy. Soc. London Ser. A* **265**, 245–263 (1962)
- Boyer, C.: The multimagic squares site, <http://www.multimagie.com>
- Boyer, C.: Some notes on the magic squares of squares problem. *Math. Intelligencer* **27**(2), 52–64 (2005)
- Bruin, N., Thomas, J., Várilly-Alvarado, A.: Explicit computation of symmetric differentials and its application to quasi-hyperbolicity. *Algebra Number Theory* **16**(6), 1377–1405 (2022)
- Brüdern, J., Wooley, T.D.: On Waring's problem for larger powers. *J. Reine Angew. Math.* **805**, 115–142 (2023)
- Cammann, S.: The evolution of magic squares in China. *J. Am. Orient. Soc.* **80**(2), 116–124 (1960)
- Derksen, H., Eggermont, C., van den Essen, A.: Multimagic squares. *Amer. Math. Monthly* **114**(8), 703–713 (2007)
- Davenport, H., Lewis, D.J.: Simultaneous equations of additive type. *Philos. Trans. Roy. Soc. London Ser. A* **264**, 557–595 (1969)
- Flores, D.: A circle method approach to k -multimagic squares. [arXiv:2406.08161](https://arxiv.org/abs/2406.08161). *Journal of the London Mathematical Society*, to appear
- Hu, C., Meng, J., Pan, F., Su, M., Xiong, S.: On the existence of a normal trimagic square of order 16 n. *J. Math.* **2023**, 1–9 (2023)
- Hu, C., Pan, F.: New infinite classes for normal trimagic squares of even orders using row-square magic rectangles. *Mathematics* **12**(8), 1194 (2024)
- Keedwell, A.D.: Gaston Tarry and multimagic squares. *Math. Gaz.* **95**(534), 454–468 (2011)
- Pan, F., Li, W., Chen, G., Xin, B.: A complete solution to the existence of normal bimagic squares of even order. *Discrete Math.* **344**(4), 112292 (2021)
- Rydin Myerson, S.L.: Quadratic forms and systems of forms in many variables. *Invent. Math.* **213**(1), 205–235 (2018)
- Rome, N., Yamagishi, S.: Integral solutions to systems of diagonal equations. [arXiv:2406.09256](https://arxiv.org/abs/2406.09256). *Pacific Journal of Mathematics*, to appear
- Schmidt, W. M.: Simultaneous rational zeros of quadratic forms, *Seminar on Number Theory, Paris 1980–81*, Progr. Math., vol. 22, Birkhäuser, Boston, MA, pp. 281–307 (1982)
- Várilly-Alvarado, A.: The geometric disposition of Diophantine equations. *Notices Amer. Math. Soc.* **68**(8), 1291–1300 (2021)
- Vaughan, R.C.: A new iterative method in Waring's problem. *Acta Math.* **162**, 1–71 (1989)
- Wooley, T.D.: Large improvements in Waring's problem. *Ann. of Math. (2)* **135**(1), 131–164 (1992)
- Wooley, T.D.: New estimates for smooth Weyl sums. *J. London Math. Soc. (2)* **51**(1), 1–13 (1995)
- Wooley, T.D.: The cubic case of the main conjecture in Vinogradov's mean value theorem. *Adv. Math.* **294**, 532–561 (2016)
- Wooley, T.D.: Nested efficient congruencing and relatives of Vinogradov's mean value theorem. *Proc. London Math. Soc. (3)* **118**(4), 942–1016 (2019)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.