Utilitas Mathematica
www.combinatorialpress.com/um

Combinatorial Press

A deterministic construction of compound pandiagonal magic squares of order k^2 via modular inverse shifts

Osamu Shimabukuro[*]

ABSTRACT

Let k be an odd prime and choose $s \in \mathbb{Z}_k^\times$ with $s^2 \not\equiv \pm 1 \pmod{k}$ (hence $k \geq 7$). We give a deterministic, purely algebraic construction of *compound pandiagonal* (Nasik) magic squares of order k^2 with consecutive entries $\{0, 1, \ldots, k^4 - 1\}$. The input is the $k \times k$ *Modular Inverse Shift* (MIS) kernel $M_s(i, j) = si + s^{-1}j \in \mathbb{Z}_k$, a classical *linear Latin square*. Our contribution is not a new Latin-square object, but a closed-form integration of: (i) orthogonality of $(M_s, M_s^\top)$, (ii) toroidal diagonal-regularity, and (iii) a two-level base-k digit superposition producing a $k^2 \times k^2$ square with closed-form evaluation of entries. We encode four $\mathbb{Z}_k$-digits coming from $(M_s, M_s^\top)$ at both the block level and the within-block level, obtaining an explicit formula $P_s(I, J) \in \{0, \ldots, k^4 - 1\}$. Orthogonality yields bijectivity, while a carry-sensitive diagonal decomposition proves that every broken diagonal of both slopes sums to the magic constant. Finally, evaluating block sums shows that the induced $k \times k$ block-sum array is itself pandiagonal magic, establishing the compound property.

Keywords: combinatorial designs, latin squares, magic squares, pandiagonal magic squares, modular arithmetic, explicit construction

2020 Mathematics Subject Classification: 05B15, 11B75, 11A07.

1. Introduction

Magic squares form a classical meeting point of arithmetic, combinatorics, and algebra. Among their many variants, *pandiagonal* (also called *Nasik* or *diabolic*) magic squares

[*] Corresponding author.

Received 30 Dec 2025; Revised 10 Jan 2026; Accepted 16 Jan 2026; Published Online 12 Feb 2026.

DOI: 10.61091/um126-06

impose particularly rigid global constraints: not only rows, columns, and the two main diagonals, but also all *broken diagonals* (with wrap-around indexing on the torus) must have the same line sum. Early systematic discussions of the wrap-around diagonal constraints go back to Frost [6], and Rosser–Walker developed an algebraic framework for diabolic squares and their transformation groups in [13, 14]. For general background, see Andrews [1] and Omori [12].

A further refinement relevant to this paper is the *compound* condition. An order k^2 magic square is called *compound* if the array can be partitioned into $k \times k$ blocks and the resulting $k \times k$ matrix of block sums is itself a magic square of order k. Compound constructions have a long history (in particular for associative/regular families), and modern discussions of such compounding mechanisms appear, for example, in the context of Frierson-type parameterizations; see Loly–Cameron [10]. From the design-theoretic viewpoint, it is natural to approach highly structured magic squares via Latin squares and orthogonality, as summarized in the *Handbook of Combinatorial Designs* [4].

Related deterministic constructions and where we sit. There exist several deterministic approaches to pandiagonal magic squares, ranging from explicit families in selected congruence classes [8] to the particularly strong *most-perfect* class [11]. On the Latin-square side, pandiagonal (Nasik) Latin squares and their orthogonality properties are also studied in connection with modular n-queens constructions and panmagic squares; see, for example, Bell–Stevens [2] and the earlier algorithmic/structural treatments such as Xu–Lu [15]. These works make clear that "pandiagonality" and "orthogonality" are classical design constraints, and that linear (affine) Latin squares over $\mathbb{Z}_k$ provide a standard source of explicit examples.

Positioning: what is not *new, and what* is *new here.* The $k \times k$ kernel underlying our construction is a *linear Latin square* over $\mathbb{Z}_k$. Thus, at the level of Latin-square theory, the kernel itself is not a new combinatorial object. The contribution of the present paper is instead at the *construction level*: we integrate a specific linear kernel with its transpose into a two-scale base-k encoding that yields, in closed form and without any search for orthogonal mates, a family of order k^2 arrays satisfying simultaneously: (i) *normality* (the entries are exactly $\{0, 1, \ldots, k^4 - 1\}$), (ii) the full *pandiagonal* condition at order k^2, and (iii) a *compound* block-sum pandiagonality property.

Why prime k and admissible parameters. We work with a prime $k \geq 5$ so that $\mathbb{Z}_k$ is a field and every nonzero residue has a unique inverse. This guarantees that the linear maps appearing in (a) diagonal-regularity of the kernel and (b) the orthogonality-with-transpose test are invertible. Equivalently, our admissible parameter range excludes the two degenerate cases where the relevant linear coefficients vanish, which in our setting reduces to a transparent condition of the form "$m \not\equiv \pm 1 \pmod{k}$". We make explicit in the body of the paper exactly which steps use field structure and which merely use unit conditions, so the role of the primality assumption is fully auditable.

Method in one sentence. We build an order k^2 square by superposing a linear Latin-square kernel and its transpose *both at the block scale and at the within-block scale* and then encoding the resulting four base-k digits as a single integer in $\{0, 1, \ldots, k^4 - 1\}$.

Technical bottleneck: global broken diagonals and carry control. While bijectivity follows cleanly from orthogonality (hence from an explicit 2 × 2 invertibility condition), pandiagonality at order k^2 requires a global analysis of broken diagonals on the $k^2 \times k^2$ torus. The key point is that lifting congruences along a global diagonal to integer equalities introduces a *carry* function. Our proof is fully explicit: each global broken diagonal sum is decomposed into four digit-level sums coming from broken diagonals of the kernel and its transpose, plus a carry contribution. We isolate the carry/no-carry counts into a short lemma showing that they depend only on the diagonal offset and not on block indices, thereby eliminating "by analogy" gaps and making the verification line-by-line.

Summary of contributions.

1. We define a concrete linear Latin-square kernel over $\mathbb{Z}_k$ and record the exact conditions under which it is pandiagonal (diagonal-regular) as a Latin square.

2. We prove that this kernel is orthogonal to its transpose under a simple arithmetic nondegeneracy condition, hence no external orthogonal-mate search is needed.

3. Using a two-scale base-k superposition, we obtain a closed-form bijection from the $k^2 \times k^2$ grid onto $\{0, 1, \ldots, k^4 - 1\}$.

4. We prove strict pandiagonality by an explicit diagonal parametrization together with a carry-sensitive decomposition, and we prove the compound property by evaluating block sums and showing the induced $k \times k$ block-sum square is pandiagonal magic.

Computational validation (supplementary). Because the construction simultaneously enforces bijectivity, pandiagonality in both slopes, and the compound block-sum condition, we also include a concise verification protocol and representative test cases computed in Magma [3], which serve as reproducible consistency checks supporting (but not replacing) the proofs.

Section 2 fixes definitions (broken diagonals on the torus, orthogonality, and the compound condition) and indexing conventions. Sections 3–4 analyze the kernel and establish orthogonality and bijectivity. Section 5 contains the carry-based pandiagonality proof for global broken diagonals. Section 6 proves the compound block-sum property. Examples and computational validation tables are presented in Section 7, followed by concluding remarks in Section 8.

2. Preliminaries and Notation

Throughout, let $k \geq 7$ be a prime. We write

$$\mathbb{Z}_k := \mathbb{Z}/k\mathbb{Z} \cong \{0, 1, \ldots, k-1\},$$

for the residue ring, always identifying an element of $\mathbb{Z}_k$ with its standard representative in $\{0, 1, \ldots, k-1\}$ when we speak about integers. Since k is prime, $\mathbb{Z}_k$ is a field, hence every nonzero element has a multiplicative inverse (cf. [9]).

2.1. Toroidal indexing and broken diagonals

Let $m \geq 1$ be an integer. An $m \times m$ *array* is a function

$$A : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}.$$

We refer to $(i,j) \in \mathbb{Z}_m \times \mathbb{Z}_m$ as the *cell* in row i and column j. All row/column/diagonal notions in this paper are *toroidal* (wrap-around) unless stated otherwise, as in the classical Nasik/diabolic framework [6, 14].

Definition 2.1 (Rows, columns, and broken diagonals)**.** Let $A : \mathbb{Z}_m^2 \to \mathbb{Z}$ be an $m \times m$ array. For $i \in \mathbb{Z}_m$ and $j \in \mathbb{Z}_m$, define the *i-th row* and *j-th column* sums by

$$R_i(A) := \sum_{t \in \mathbb{Z}_m} A(i,t), \qquad C_j(A) := \sum_{t \in \mathbb{Z}_m} A(t,j).$$

For $a \in \mathbb{Z}_m$, define the *broken diagonals* of slopes $+1$ and -1 by

$$D_a^+ := \{(t,\, t+a) \in \mathbb{Z}_m^2 \mid t \in \mathbb{Z}_m\}, \qquad D_a^- := \{(t,\, -t+a) \in \mathbb{Z}_m^2 \mid t \in \mathbb{Z}_m\},$$

and their sums by

$$\Delta_a^+(A) := \sum_{(i,j) \in D_a^+} A(i,j), \qquad \Delta_a^-(A) := \sum_{(i,j) \in D_a^-} A(i,j).$$

Definition 2.2 (Pandiagonal (Nasik/diabolic) magic square)**.** An $m \times m$ array $A : \mathbb{Z}_m^2 \to \mathbb{Z}$ is a *pandiagonal magic square* if there exists an integer μ such that

$$R_i(A) = \mu \quad (\forall i \in \mathbb{Z}_m), \qquad C_j(A) = \mu \quad (\forall j \in \mathbb{Z}_m), \qquad \Delta_a^{\pm}(A) = \mu \quad (\forall a \in \mathbb{Z}_m).$$

If, moreover, the multiset of entries is exactly $\{0, 1, \dots, m^2 - 1\}$, then A is said to be *normal*.

The terminology "Nasik" and "diabolic" for the wrap-around diagonal condition appears in early sources such as [6, 14]; we follow the now common term *pandiagonal*.

Proposition 2.3 (Magic constant for normal squares)**.** *Let A be a normal $m \times m$ pandiagonal magic square in the sense of Definition 2.2. Then its magic constant is*

$$\mu = \frac{m(m^2 - 1)}{2}.$$

Proof. Since A is normal, the total sum of all entries equals

$$\sum_{x=0}^{m^2-1} x = \frac{m^2(m^2 - 1)}{2}.$$

On the other hand, this total sum also equals $\sum_{i \in \mathbb{Z}_m} R_i(A) = m\mu$. Dividing by m gives $\mu = \frac{m(m^2-1)}{2}$. □

2.2. Latin squares, orthogonality, and linear models

We use Latin squares as the algebraic "digit" devices underlying the construction (cf. standard references [5, 4]).

Definition 2.4 (Latin square)**.** A *Latin square of order k* on the symbol set $\mathbb{Z}_k$ is a map

$$L : \mathbb{Z}_k \times \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$$

such that, for every fixed $i \in \mathbb{Z}_k$, the map $j \mapsto L(i,j)$ is a bijection of $\mathbb{Z}_k$, and for every fixed $j \in \mathbb{Z}_k$, the map $i \mapsto L(i,j)$ is a bijection of $\mathbb{Z}_k$.

Definition 2.5 (Orthogonality)**.** Two Latin squares $L_1, L_2 : \mathbb{Z}_k^2 \to \mathbb{Z}_k$ are *orthogonal* if the map

$$\mathbb{Z}_k^2 \longrightarrow \mathbb{Z}_k^2, \qquad (i,j) \longmapsto (L_1(i,j),\, L_2(i,j)),$$

is a bijection. Equivalently, each ordered pair in $\mathbb{Z}_k^2$ occurs exactly once among the superimposed entries. (See [5, 4].)

Definition 2.6 (Toroidal diagonal-regularity for a Latin square)**.** Let $L : \mathbb{Z}_k^2 \to \mathbb{Z}_k$ be a Latin square. We say that L is *toroidally diagonal-regular* if, for every $a \in \mathbb{Z}_k$, the restrictions $t \mapsto L(t, t+a)$ and $t \mapsto L(t, -t+a)$ are bijections $\mathbb{Z}_k \to \mathbb{Z}_k$.

Diagonal constraints for Latin squares (in various forms) are classical and appear in the Latin-square literature; Definition 2.6 is the toroidal form tailored to pandiagonality [5, 4].

Definition 2.7 (Linear Latin square)**.** For $a, b \in \mathbb{Z}_k$, define

$$L_{a,b}(i,j) := ai + bj \in \mathbb{Z}_k \qquad (i, j \in \mathbb{Z}_k).$$

We call $L_{a,b}$ a *linear Latin square* (over $\mathbb{Z}_k$).

Linear Latin squares are a standard family [7, 5]. The next propositions record the exact nondegeneracy conditions we shall use.

Proposition 2.8 (Latin property and diagonal-regularity)**.** *Let $a, b \in \mathbb{Z}_k$. Then:*

(i) *$L_{a,b}$ is a Latin square if and only if $a \neq 0$ and $b \neq 0$ in $\mathbb{Z}_k$.*

(ii) *If $a, b \neq 0$ and $a \pm b \neq 0$, then $L_{a,b}$ is toroidally diagonal-regular in the sense of Definition 2.6.*

Proof. (i) Fix $i \in \mathbb{Z}_k$. Then $j \mapsto L_{a,b}(i,j) = ai + bj$ is a bijection if and only if $b \neq 0$. Similarly, fixing j yields bijectivity in i if and only if $a \neq 0$. Thus $L_{a,b}$ is Latin exactly when $a, b \neq 0$.

(ii) Assume $a, b \neq 0$. For each $c \in \mathbb{Z}_k$, consider the slope $+1$ diagonal map

$$t \longmapsto L_{a,b}(t, t+c) = (a+b)t + bc.$$

This is a bijection if and only if $a+b \neq 0$. Likewise, the slope -1 diagonal map is

$$t \longmapsto L_{a,b}(t, -t+c) = (a-b)t + bc,$$

which is a bijection if and only if $a-b \neq 0$. In our application (MIS kernel), the parameters are chosen so that $a \pm b \neq 0$ holds. Under this condition, both families of broken diagonals are permutations, hence $L_{a,b}$ is diagonal-regular. □

Remark 2.9. In later sections the MIS kernel will be a specific $L_{a,b}$ arising from a modular inverse. The parameter restriction used in the main theorem implies $a \pm b \neq 0$ in $\mathbb{Z}_k$, so Proposition 2.8(ii) applies.

Proposition 2.10 (Orthogonality of linear Latin squares)**.** *Let $a, b, c, d \in \mathbb{Z}_k$ with $a, b, c, d \neq 0$. Then $L_{a,b}$ and $L_{c,d}$ are orthogonal (Definition 2.5) if and only if*

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq 0 \quad \text{in } \mathbb{Z}_k.$$

Proof. Consider the map $\Phi : \mathbb{Z}_k^2 \to \mathbb{Z}_k^2$ given by

$$\Phi(i,j) = (L_{a,b}(i,j),\, L_{c,d}(i,j)) = (ai + bj,\, ci + dj).$$

This is $\mathbb{Z}_k$-linear with matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Over the field $\mathbb{Z}_k$ the map Φ is bijective if and only if its determinant is nonzero. By Definition 2.5, bijectivity of Φ is exactly orthogonality. □

Corollary 2.11 (Orthogonality with the transpose)**.** *Let $a, b \in \mathbb{Z}_k$ with $a, b \neq 0$, and write $L := L_{a,b}$. Then L is orthogonal to its transpose $L^{\mathsf{T}}(i,j) := L(j,i) = aj + bi$ if and only if*

$$a^2 - b^2 \neq 0 \quad \text{in } \mathbb{Z}_k, \qquad (\text{equivalently, } a \not\equiv \pm b \pmod{k}).$$

Proof. Let $a, b \in \mathbb{Z}_k^\times$ and consider the two linear Latin squares $L_{a,b}(i,j) = ai + bj$ and its transpose $L_{b,a}(i,j) = bi + aj$. Define a $\mathbb{Z}_k$-linear map

$$\Phi : \mathbb{Z}_k^2 \to \mathbb{Z}_k^2, \qquad \Phi(i,j) = (L_{a,b}(i,j),\, L_{b,a}(i,j)) = (ai + bj,\, bi + aj).$$

By Definition 2.5, the pair $(L_{a,b}, L_{b,a})$ is orthogonal if and only if Φ is bijective.

The matrix of Φ is $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, whose determinant equals

$$\det \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a^2 - b^2 = (a-b)(a+b) \in \mathbb{Z}_k.$$

Since $\mathbb{Z}_k$ is a field, Φ is bijective if and only if this determinant is nonzero, i.e. if and only if $a \not\equiv \pm b \pmod{k}$. □

2.3. Base-k digit notation and superposition

A key feature of the construction is a closed-form *digit superposition* that turns a small number of $\mathbb{Z}_k$-valued "digits" into a single integer entry (cf. the general compound constructions surveyed in [1, 10]).

Definition 2.12 (Base-k encoding)**.** Define the map

$$\mathrm{enc}_k : \mathbb{Z}_k^4 \longrightarrow \{0, 1, \dots, k^4 - 1\} \subset \mathbb{Z},$$

by

$$\mathrm{enc}_k(d_0, d_1, d_2, d_3) := d_0 + kd_1 + k^2 d_2 + k^3 d_3,$$

where each $d_r \in \mathbb{Z}_k$ is identified with its representative in $\{0, 1, \dots, k - 1\}$.

Proposition 2.13 (Encoding bijection)**.** *The map* enc_k *in Definition 2.12 is a bijection. Equivalently, each integer* $x \in \{0, 1, \dots, k^4 - 1\}$ *admits a unique base-k expansion*

$$x = d_0 + kd_1 + k^2 d_2 + k^3 d_3, \qquad d_r \in \{0, 1, \dots, k - 1\}.$$

Proof. This is the standard uniqueness of base-k expansions. Injectivity: if $\sum_{r=0}^{3} k^r d_r = \sum_{r=0}^{3} k^r d'_r$ with $0 \le d_r, d'_r \le k - 1$, reduce modulo k to get $d_0 = d'_0$, subtract and divide by k, and iterate. Surjectivity: given x, define $d_0 \equiv x \pmod{k}$ with $0 \le d_0 \le k - 1$, then set $x_1 = (x - d_0)/k$ and repeat. □

Definition 2.14 (Block digits for indices in $\mathbb{Z}_{k^2}$)**.** For $I \in \mathbb{Z}_{k^2}$, define its *digits* $(i_0, i_1) \in \mathbb{Z}_k^2$ by the unique decomposition

$$I \equiv i_0 + ki_1 \pmod{k^2} \qquad \text{with } i_0, i_1 \in \{0, 1, \dots, k - 1\}.$$

We write $I \leftrightarrow (i_0, i_1)$, and similarly $J \leftrightarrow (j_0, j_1)$.

Remark 2.15. Under Definition 2.14, the pair $(i_1, j_1) \in \mathbb{Z}_k^2$ records the *block* of size $k \times k$ containing the cell $(I, J) \in \mathbb{Z}_{k^2}^2$, while (i_0, j_0) records the position *within* that block. This is the formal basis of the compound property.

Definition 2.16 (Base-k superposition of digit arrays)**.** Let $D_0, D_1, D_2, D_3 : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}_k$ be $\mathbb{Z}_k$-valued digit arrays. Their *base-k superposition* is the integer array

$$S : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}, \qquad S(I, J) := \mathrm{enc}_k\left(D_0(I, J), D_1(I, J), D_2(I, J), D_3(I, J)\right).$$

Proposition 2.17 (Bijection criterion via digit tuples)**.** *With notation as in Definition 2.16, the following are equivalent:*

(i) *The superposition S is normal, i.e. its entries are exactly* $\{0, 1, \dots, k^4 - 1\}$*.*

(ii) *The map*

$$\Psi : \mathbb{Z}_{k^2}^2 \longrightarrow \mathbb{Z}_k^4, \qquad (I,J) \longmapsto \left(D_0(I,J), D_1(I,J), D_2(I,J), D_3(I,J)\right),$$

is a bijection.

Proof. By Proposition 2.13, enc_k is a bijection from $\mathbb{Z}_k^4$ to $\{0,1,\dots,k^4-1\}$. Hence $S = \mathrm{enc}_k \circ \Psi$ is a bijection onto $\{0,1,\dots,k^4-1\}$ if and only if Ψ is a bijection onto $\mathbb{Z}_k^4$. □

2.4. Compound pandiagonal magic squares

We finally formalize the compound condition used in the main theorem (cf. [1, 10]).

Definition 2.18 (Block sums and compound property)**.** Let $A : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}$ be a $k^2 \times k^2$ array. For each block index $(u,v) \in \mathbb{Z}_k^2$, define the (u,v)*-block*

$$B_{u,v} := \{(I,J) \in \mathbb{Z}_{k^2}^2 : \ I \leftrightarrow (i_0,u), \ J \leftrightarrow (j_0,v) \text{ for some } (i_0,j_0) \in \mathbb{Z}_k^2\},$$

and its *block sum*

$$\Sigma_{u,v}(A) := \sum_{(I,J)\in B_{u,v}} A(I,J).$$

The *block-sum array* is the $k \times k$ array

$$\Sigma(A) : \mathbb{Z}_k^2 \to \mathbb{Z}, \qquad \Sigma(A)(u,v) := \Sigma_{u,v}(A).$$

We say that A is *compound pandiagonal magic* if

(i) A is pandiagonal magic of order k^2 (Definition 2.2), and

(ii) the block-sum array $\Sigma(A)$ is pandiagonal magic of order k (with respect to toroidal broken diagonals on $\mathbb{Z}_k^2$).

Remark 2.19. Condition (ii) in Definition 2.18 asserts that the “macroscopic” $k \times k$ pattern of block totals is itself a pandiagonal magic square. This is the precise sense in which the order k^2 square carries a nontrivial hierarchical (purely algebraic) regularity beyond pandiagonality.

2.5. Summary of notation

We follow the standard conventions for toroidal indexing and Latin-square terminology; see, e.g., [5, 4].

The notions usind throughout this paper are presented in Table 1 and schematic view of the $k \times k$ block structure and digit decomposition is presented in Figure 1.

Table 1. Notation used throughout the paper

Symbol	Meaning
$\mathbb{Z}_m$	integers modulo m (toroidal indexing)
k	a prime modulus (typically $k \geq 7$; see Remark 7.2)
$\mathbb{Z}_k^\times$	the unit group of $\mathbb{Z}_k$
$s \in \mathbb{Z}_k^\times$	MIS parameter; admissible if $s^2 \not\equiv \pm 1 \pmod{k}$
$M_s(i,j)$	MIS kernel $= si + s^{-1}j \in \mathbb{Z}_k$
$I, J \in \mathbb{Z}_{k^2}$	global indices of the $k^2 \times k^2$ square
$i_0, i_1, j_0, j_1 \in \mathbb{Z}_k$	digits: $I \equiv i_0 + ki_1$, $J \equiv j_0 + kj_1$
$D_0, \ldots, D_3$	digit arrays used in the base-k encoding
$P_s(I,J)$	encoded square of order k^2 (Construction 4.7)
$\Sigma(P_s)$	block-sum array of order k (Definition 6.1)

Global/local index decomposition (order k^2)

$$I \in \mathbb{Z}_{k^2} \;\leftrightarrow\; (i_0, i_1) \in \mathbb{Z}_k^2, \qquad J \in \mathbb{Z}_{k^2} \;\leftrightarrow\; (j_0, j_1) \in \mathbb{Z}_k^2$$

$$I \equiv i_0 + ki_1, \qquad J \equiv j_0 + kj_1$$

$$\boxed{\text{block index } (i_1, j_1) \in \mathbb{Z}_k^2} \quad + \quad \boxed{\text{within-block index } (i_0, j_0) \in \mathbb{Z}_k^2}$$

Fig. 1. Schematic view of the $k \times k$ block structure and digit decomposition

3. The MIS kernel and its properties

Throughout this section, $k \geq 7$ is a fixed prime and $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$ is identified with $\{0, 1, \ldots, k-1\}$ as in Section 2. We recall that our "MIS kernel" is not claimed to be a new combinatorial object: it is a particular *linear Latin square* over $\mathbb{Z}_k$ in the sense of Definition 2.7, i.e. a classical family studied in, e.g., [7, 5]. The novelty lies in the way this kernel is integrated into a closed-form compound pandiagonal magic-square construction (cf. Introduction).

3.1. *Definition of the MIS kernel*

We parameterize the kernel by a nonzero slope parameter $s \in \mathbb{Z}_k^\times$. Since k is prime, s has a unique inverse $s^{-1} \in \mathbb{Z}_k^\times$ (cf. [9]).

Definition 3.1 (MIS kernel)**.** Let $s \in \mathbb{Z}_k^\times$. Define the *MIS kernel* associated with s to be the $k \times k$ array

$$M_s : \mathbb{Z}_k \times \mathbb{Z}_k \longrightarrow \mathbb{Z}_k, \qquad M_s(i,j) := s\,i + s^{-1}j.$$

We also write $M_s^{\mathsf{T}}(i,j) := M_s(j,i)$ for its transpose.

Remark 3.2 (Linear Latin-square interpretation)**.** By Definition 2.7,

$$M_s = L_{a,b} \quad \text{with} \quad a = s,\ b = s^{-1}.$$

Hence M_s belongs to the classical class of linear Latin squares [7, 5]. The term "MIS" is convenient shorthand for the specific inverse-coupled choice $(a, b) = (s, s^{-1})$.

3.2. Latin property and diagonal regularity

Proposition 3.3 (Latin property)**.** *For every $s \in \mathbb{Z}_k^\times$, the MIS kernel M_s is a Latin square of order k on $\mathbb{Z}_k$.*

Proof. Fix $i \in \mathbb{Z}_k$. Then the map $j \mapsto M_s(i,j) = s\,i + s^{-1}j$ is an affine linear map with nonzero coefficient s^{-1}, hence a bijection of $\mathbb{Z}_k$. Similarly, for fixed j, the map $i \mapsto s\,i + s^{-1}j$ has nonzero coefficient s, hence is bijective. Therefore M_s is Latin by Definition 2.4. (Equivalently, apply Proposition 2.8(i) to $a = s$, $b = s^{-1}$.) □

Definition 3.4 (Diagonal-regular MIS parameter)**.** We say that $s \in \mathbb{Z}_k^\times$ is *diagonal-regular* if

$$s^2 \not\equiv \pm 1 \pmod{k}, \quad \text{i.e.} \quad s^2 - 1 \neq 0 \text{ and } s^2 + 1 \neq 0 \text{ in } \mathbb{Z}_k.$$

Proposition 3.5 (Toroidal diagonal-regularity)**.** *If $s \in \mathbb{Z}_k^\times$ is diagonal-regular (Definition 3.4), then M_s is toroidally diagonal-regular in the sense of Definition 2.6. Equivalently, for each $a \in \mathbb{Z}_k$, the maps*

$$t \longmapsto M_s(t, t+a), \qquad t \longmapsto M_s(t, -t+a),$$

are permutations of $\mathbb{Z}_k$.

Proof. Compute, for fixed $a \in \mathbb{Z}_k$,

$$M_s(t, t+a) = s\,t + s^{-1}(t+a) = (s + s^{-1})t + s^{-1}a,$$

$$M_s(t, -t+a) = s\,t + s^{-1}(-t+a) = (s - s^{-1})t + s^{-1}a.$$

Each is an affine linear map $t \mapsto \alpha t + \beta$ on $\mathbb{Z}_k$, hence bijective if and only if $\alpha \neq 0$. Now $\alpha = s + s^{-1} = 0$ is equivalent to $s^2 + 1 = 0$ in $\mathbb{Z}_k$, and $\alpha = s - s^{-1} = 0$ is equivalent to $s^2 - 1 = 0$ in $\mathbb{Z}_k$. Thus diagonal-regularity of s implies both coefficients are nonzero, proving the claim. This is a specialization of Proposition 2.8(ii) to $(a, b) = (s, s^{-1})$. □

Remark 3.6 (Relation to diabolic/Nasik constraints)**.** The diagonal-regularity in Proposition 3.5 is the Latin-square analogue of the wrap-around diagonal constraints for diabolic (pandiagonal) structures [6, 14]. In our later superposition, this property is the mechanism by which pandiagonality is inherited.

3.3. Orthogonality with the transpose

Orthogonality of Latin squares is a standard notion [5, 4]. For linear Latin squares, it reduces to a determinant condition, as recalled in Proposition 2.10. The present kernel is designed so that orthogonality can be checked by a single congruence in s.

Proposition 3.7 (Orthogonality of M_s and M_s^{T})**.** *Let $s \in \mathbb{Z}_k^{\times}$. Then M_s is orthogonal to its transpose M_s^{T} if and only if*

$$s^4 \not\equiv 1 \pmod{k} \qquad \textit{equivalently} \qquad s^2 \not\equiv \pm 1 \pmod{k}.$$

Proof. By Remark 3.2, $M_s = L_{s,s^{-1}}$ and $M_s^{\mathsf{T}} = L_{s^{-1},s}$. Apply Proposition 2.10: M_s and M_s^{T} are orthogonal if and only if

$$\det \begin{pmatrix} s & s^{-1} \\ s^{-1} & s \end{pmatrix} = s^2 - s^{-2} \neq 0 \quad \text{in } \mathbb{Z}_k.$$

Multiplying by $s^2 \neq 0$ yields the equivalent condition $s^4 - 1 \neq 0$ in $\mathbb{Z}_k$, i.e. $s^4 \not\equiv 1 \pmod{k}$. Since $s^4 - 1 = (s^2 - 1)(s^2 + 1)$ in $\mathbb{Z}_k$, this is equivalent to $s^2 \not\equiv \pm 1 \pmod{k}$. □

Corollary 3.8 (A unified admissibility condition)**.** *Let $s \in \mathbb{Z}_k^{\times}$. If $s^2 \not\equiv \pm 1 \pmod{k}$, then:*

(i) *M_s is a Latin square (Proposition 3.3);*
(ii) *M_s is toroidally diagonal-regular (Proposition 3.5);*
(iii) *M_s is orthogonal to M_s^{T} (Proposition 3.7).*

Remark 3.9. Assume that k is an odd prime and set

$$S_k = \{\, s \in \mathbb{Z}_k^{\times} \mid s^2 \not\equiv \pm 1 \pmod{k} \,\}.$$

Then $S_k \neq \varnothing$ for every prime $k \geq 7$. Moreover, the exact cardinality of S_k is given in Proposition 7.1 (and depends on whether -1 is a quadratic residue modulo k). For completeness, note that for $k = 5$ every nonzero square is ± 1, hence $S_5 = \varnothing$.

3.4. Permutation viewpoint and random access

The next reformulation makes explicit how the kernel encodes permutations, a viewpoint that is standard in Latin-square theory [5] and is convenient for our later "random access" evaluation.

Proposition 3.10 (Row and column permutations)**.** *Let $s \in \mathbb{Z}_k^{\times}$. For each $i \in \mathbb{Z}_k$, the row map*

$$\pi_i : \mathbb{Z}_k \to \mathbb{Z}_k, \qquad \pi_i(j) := M_s(i,j),$$

is a permutation of $\mathbb{Z}_k$, and for each $j \in \mathbb{Z}_k$, the column map

$$\rho_j : \mathbb{Z}_k \to \mathbb{Z}_k, \qquad \rho_j(i) := M_s(i,j),$$

is a permutation of $\mathbb{Z}_k$. Moreover, each is an affine permutation:

$$\pi_i(j) = s^{-1}j + (s\,i), \qquad \rho_j(i) = s\,i + (s^{-1}j).$$

Proof. This is immediate from the explicit formula $M_s(i,j) = s\,i + s^{-1}j$ and the fact that multiplication by a nonzero element in $\mathbb{Z}_k$ is a bijection [9]. It also restates Proposition 3.3. □

Remark 3.11 (Why this matters later)**.** In the full order k^2 construction, each entry will be an explicit base-k encoding of four $\mathbb{Z}_k$-digits, each digit being an affine expression in the corresponding index digits (Definition 2.14). Proposition 3.10 is the elementary mechanism behind this "random access": no search is required to recover the digit values.

3.5. Worked example

Example 3.12 (A small kernel)**.** Let $k = 7$ and choose $s = 2 \in \mathbb{Z}_7^\times$. Then $s^{-1} = 4$ in $\mathbb{Z}_7^\times$ and the MIS kernel is

$$M_2(i,j) = 2i + 4j \pmod 7.$$

Since $s^2 = 4 \not\equiv \pm 1 \pmod 7$, the parameter is admissible: M_2 is diagonal-regular and orthogonal to its transpose by Corollary 3.8.

3.6. Where the field (prime) hypothesis is used

Latin-square properties of linear forms and their orthogonality criteria are classical; see [5, 4]. We record, for clarity, the precise dependence of our arguments on invertibility in $\mathbb{Z}_k$.

Remark 3.13 (Dependency table: unit vs. field)**.** Throughout, k is assumed prime so that $\mathbb{Z}_k$ is a field. Conceptually, however, the proofs use only the following invertibility facts.

(1) *Kernel Latin property:* for $L_{a,b}(i,j) = ai + bj$ to be Latin, it suffices that a, b are units in the coefficient ring (so that $i \mapsto ai + c$ and $j \mapsto bj + c$ are bijections); this is standard [5, 4].

(2) *Orthogonality of two linear Latin squares:* for $L_{a,b}$ and $L_{c,d}$, the condition

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0,$$

ensures orthogonality over a field; in our prime setting this is equivalent to being a unit and is used to guarantee the digit-map bijection in Section 4 [5, 4].

(3) *MIS specialization:* in $M_s(i,j) = si + s^{-1}j$, the inverse s^{-1} requires $s \in \mathbb{Z}_k^\times$. The unified admissibility condition $s^2 \not\equiv \pm 1 \pmod k$ then simultaneously enforces (i) diagonal-regularity (for pandiagonality) and (ii) orthogonality with the transpose (for normality).

(4) *Carry/borrow analysis:* the carry/borrow lemmas use only standard representatives $\{0, 1, \dots, k-1\}$ and integer inequalities, and do not require additional field structure.

4. Orthogonality and base-k encoding

In this section we explain how orthogonality of the MIS kernel with its transpose yields a *bijective digit map*, and how a base-k encoding then produces a normal $k^2 \times k^2$ square with entries $\{0, 1, \ldots, k^4 - 1\}$. The underlying principles are standard in Latin-square theory [5, 4] and positional numeral systems.

Throughout, $k \geq 7$ is a prime and $s \in \mathbb{Z}_k^\times$ is a parameter. We use the index-digit decomposition $I \leftrightarrow (i_0, i_1)$, $J \leftrightarrow (j_0, j_1)$ from Definition 2.14.

4.1. A two-level digit system

The compound construction will superpose four $\mathbb{Z}_k$-valued digits: two digits coming from the *block indices* (i_1, j_1), and two digits coming from the *within-block indices* (i_0, j_0). Each pair of digits is produced by superposing the MIS kernel M_s and its transpose. This is the precise algebraic meaning of "no search": orthogonality implies that the pair of digits ranges over all of $\mathbb{Z}_k^2$ exactly once.

Definition 4.1 (Kernel pair map)**.** Let M_s be the MIS kernel (Definition 3.1). Define the *kernel pair map*

$$\Phi_s : \mathbb{Z}_k^2 \longrightarrow \mathbb{Z}_k^2, \qquad \Phi_s(i,j) := \big(M_s(i,j),\, M_s^\mathsf{T}(i,j)\big)\,.$$

Lemma 4.2 (Orthogonality $\Leftrightarrow$ bijectivity of Φ_s)**.** *The following are equivalent:*

(i) *M_s is orthogonal to M_s^T (Definition 2.5);*

(ii) *Φ_s is a bijection $\mathbb{Z}_k^2 \to \mathbb{Z}_k^2$.*

In this case, for every $(u,v) \in \mathbb{Z}_k^2$ there exists a unique $(i,j) \in \mathbb{Z}_k^2$ such that $\Phi_s(i,j) = (u,v)$.

Proof. By Definition 2.5, orthogonality of M_s and M_s^T means exactly that the superposition map $(i,j) \mapsto (M_s(i,j), M_s^\mathsf{T}(i,j))$ hits every ordered pair in $\mathbb{Z}_k^2$ exactly once. This is the bijectivity of Φ_s. (See [5, 4] for the standard equivalence.) □

Corollary 4.3 (Explicit admissibility condition)**.** *If $s \in \mathbb{Z}_k^\times$ satisfies $s^2 \not\equiv \pm 1 \pmod{k}$, then Φ_s is a bijection.*

Proof. By Proposition 3.7, the congruence $s^2 \not\equiv \pm 1$ is equivalent to orthogonality of M_s and M_s^T. Now apply Lemma 4.2. □

4.2. Digit arrays on $\mathbb{Z}_{k^2}^2$

We now lift the kernel-pair mechanism to the $k^2 \times k^2$ index set. The point is that each cell $(I, J) \in \mathbb{Z}_{k^2}^2$ carries two independent pairs of digits: one from the block coordinates (i_1, j_1) and one from the within-block coordinates (i_0, j_0).

Construction 4.4 (Four digit arrays). Fix $s \in \mathbb{Z}_k^\times$. For $(I, J) \in \mathbb{Z}_{k^2}^2$, write $I \leftrightarrow (i_0, i_1)$ and $J \leftrightarrow (j_0, j_1)$ as in Definition 2.14. Define digit arrays $D_0, D_1, D_2, D_3 : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}_k$ by

$$\begin{aligned}(D_0(I,J), D_1(I,J)) &:= \Phi_s(i_0, j_0),\\ (D_2(I,J), D_3(I,J)) &:= \Phi_s(i_1, j_1).\end{aligned}$$

Equivalently,

$$(D_0, D_1)(I, J) = \left(M_s(i_0, j_0),\, M_s^{\mathsf{T}}(i_0, j_0)\right), \qquad (D_2, D_3)(I, J) = \left(M_s(i_1, j_1),\, M_s^{\mathsf{T}}(i_1, j_1)\right).$$

Remark 4.5. The pair (D_0, D_1) depends only on the within-block digits (i_0, j_0), while (D_2, D_3) depends only on the block digits (i_1, j_1). This separation is what later enables the compound block-sum analysis.

Lemma 4.6 (Digit-pair bijectivity on each level). *Assume* $s^2 \not\equiv \pm 1 \pmod{k}$. *Then:*
(i) *as* (i_0, j_0) *ranges over* $\mathbb{Z}_k^2$, *the pair* (D_0, D_1) *ranges over* $\mathbb{Z}_k^2$ *bijectively;*
(ii) *as* (i_1, j_1) *ranges over* $\mathbb{Z}_k^2$, *the pair* (D_2, D_3) *ranges over* $\mathbb{Z}_k^2$ *bijectively.*

Proof. Under the hypothesis, Φ_s is a bijection by Corollary 4.3. By Construction 4.4, $(D_0, D_1) = \Phi_s(i_0, j_0)$ and $(D_2, D_3) = \Phi_s(i_1, j_1)$. Hence each claim follows by applying bijectivity of Φ_s at the corresponding level. □

4.3. Base-k encoding and normality

We now package the four digits into a single integer by a base-k encoding (Definition 2.12). This is the closed-form "superposition" step, and it is the source of random-access evaluation.

Construction 4.7 (Encoded entry function). With digit arrays from Construction 4.4, define

$$P_s : \mathbb{Z}_{k^2}^2 \longrightarrow \mathbb{Z}, \qquad P_s(I, J) := \mathrm{enc}_k\left(D_0(I,J), D_1(I,J), D_2(I,J), D_3(I,J)\right),$$

where enc_k is as in Definition 2.12. We call P_s the *encoded square* associated with s.

Proposition 4.8 (Digit-tuple bijectivity implies normality). *Assume* $s^2 \not\equiv \pm 1 \pmod{k}$. *Then the encoded square* P_s *is* normal *in the sense of Definition 2.2: its entries are exactly the set* $\{0, 1, \ldots, k^4 - 1\}$, *each appearing once.*

Proof. Consider the digit-tuple map

$$\Psi_s : \mathbb{Z}_{k^2}^2 \longrightarrow \mathbb{Z}_k^4, \qquad \Psi_s(I, J) := \left(D_0(I,J), D_1(I,J), D_2(I,J), D_3(I,J)\right).$$

By Proposition 2.17, it suffices to show that Ψ_s is a bijection.

Write $(I, J) \leftrightarrow (i_0, i_1, j_0, j_1)$ via Definition 2.14. Under the natural identification $\mathbb{Z}_{k^2}^2 \cong \mathbb{Z}_k^4$ given by

$$(I, J) \longleftrightarrow (i_0, j_0, i_1, j_1).$$

Construction 4.4 yields the factorization

$$\Psi_s(i_0, j_0, i_1, j_1) = (\Phi_s(i_0, j_0),\ \Phi_s(i_1, j_1)) \in \mathbb{Z}_k^2 \times \mathbb{Z}_k^2.$$

By Corollary 4.3, Φ_s is a bijection of $\mathbb{Z}_k^2$. Hence the product map $(x, y) \mapsto (\Phi_s(x), \Phi_s(y))$ is a bijection of $\mathbb{Z}_k^2 \times \mathbb{Z}_k^2$, so Ψ_s is a bijection of $\mathbb{Z}_k^4$. Therefore P_s is normal. □

Remark 4.9 (Random access)**.** The formula in Construction 4.7 expresses $P_s(I, J)$ directly in terms of the index digits (i_0, i_1, j_0, j_1) through affine maps in $\mathbb{Z}_k$ and a base-k encoding. Thus any entry can be computed without constructing the full square, which is a key algorithmic feature emphasized in the Introduction.

4.4. *Explicit closed form for the digits*

For later use, we record the digits D_r in explicit algebraic form. This makes the dependence on s and on the index digits transparent.

Proposition 4.10 (Closed-form expressions)**.** *Let $s \in \mathbb{Z}_k^\times$ and $(I, J) \in \mathbb{Z}_{k^2}^2$ with $I \leftrightarrow (i_0, i_1)$, $J \leftrightarrow (j_0, j_1)$. Then the digits in Construction 4.4 satisfy*

$$D_0(I, J) = s\, i_0 + s^{-1} j_0, \qquad D_1(I, J) = s\, j_0 + s^{-1} i_0,$$
$$D_2(I, J) = s\, i_1 + s^{-1} j_1, \qquad D_3(I, J) = s\, j_1 + s^{-1} i_1,$$

all in $\mathbb{Z}_k$. Consequently,

$$P_s(I, J) = \left(s\, i_0 + s^{-1} j_0\right) + k\left(s\, j_0 + s^{-1} i_0\right) + k^2\left(s\, i_1 + s^{-1} j_1\right) + k^3\left(s\, j_1 + s^{-1} i_1\right),$$

where each $\mathbb{Z}_k$ digit is identified with its representative in $\{0, 1, \ldots, k-1\}$.

Proof. This is immediate from the definition of M_s (Definition 3.1) and the rule $(D_0, D_1) = \Phi_s(i_0, j_0)$, $(D_2, D_3) = \Phi_s(i_1, j_1)$ in Construction 4.4, together with the encoding definition (Definition 2.12). □

Remark 4.11 (What remains)**.** By Proposition 4.8, orthogonality already guarantees that P_s is a normal $k^2 \times k^2$ square. The remaining work toward the main theorem is to prove that P_s is pandiagonal magic and then compound pandiagonal magic (Definition 2.18), which requires a carry-sensitive analysis of broken diagonal sums.

5. Pandiagonality of the encoded square

In this section we prove that the encoded square P_s from Construction 4.7 is a *pandiagonal* (Nasik/diabolic) magic square in the toroidal sense of Definition 2.2. The wrap-around diagonal viewpoint goes back to early work such as [6] and the algebraic treatment of diabolic squares [14]. Our argument is elementary but must track the interaction between *base-k digits* and *toroidal diagonals.*

5.1. Standing assumptions and a digit-sum lemma

Fix a prime $k \geq 7$ and a parameter $s \in \mathbb{Z}_k^\times$ satisfying

$$s^2 \not\equiv \pm 1 \pmod{k}.$$

By Corollary 3.8, the MIS kernel M_s is Latin, toroidally diagonal-regular, and orthogonal to its transpose. Hence P_s is normal by Proposition 4.8. We will show that P_s is pandiagonal magic.

For $x \in \mathbb{Z}_k$, let $\widetilde{x} \in \{0, 1, \dots, k-1\}$ denote its standard representative. By Proposition 4.10, each entry $P_s(I, J)$ has the form

$$P_s(I,J) = \widetilde{D_0(I,J)} + k\,\widetilde{D_1(I,J)} + k^2\,\widetilde{D_2(I,J)} + k^3\,\widetilde{D_3(I,J)}. \tag{1}$$

For $r = 0, 1, 2, 3$, write $D^r(I,J) := \widetilde{D_r(I,J)} \in \{0, 1, \dots, k-1\}$.

Lemma 5.1 (Sum of a permuted digit set)**.** *Let $\sigma : \mathbb{Z}_k \to \mathbb{Z}_k$ be a bijection. Then*

$$\sum_{t \in \mathbb{Z}_k} \widetilde{\sigma(t)} = \sum_{u=0}^{k-1} u = \frac{k(k-1)}{2}.$$

Proof. Since σ is bijective, the multiset $\{\sigma(t) \mid t \in \mathbb{Z}_k\}$ equals $\mathbb{Z}_k$. Taking standard representatives yields the multiset $\{0, 1, \dots, k-1\}$, hence the sum is $\sum_{u=0}^{k-1} u = \frac{k(k-1)}{2}$. □

We will repeatedly use the following consequence: if $f : \mathbb{Z}_k \to \mathbb{Z}_k$ is bijective, then $\sum_{t \in \mathbb{Z}_k} \widetilde{f(t)} = \frac{k(k-1)}{2}$; if moreover each value of f occurs with multiplicity k in a sum indexed by $\mathbb{Z}_k^2$, then the total sum is $k \cdot \frac{k(k-1)}{2} = \frac{k^2(k-1)}{2}$.

5.2. Row and column sums

Proposition 5.2 (Row sums)**.** *For each fixed $I \in \mathbb{Z}_{k^2}$,*

$$\sum_{J \in \mathbb{Z}_{k^2}} P_s(I,J) = \frac{k^2(k^4-1)}{2}.$$

Proof. Fix $I \in \mathbb{Z}_{k^2}$ and write $I \leftrightarrow (i_0, i_1)$. As J ranges over $\mathbb{Z}_{k^2}$, its digits $(j_0, j_1) \in \mathbb{Z}_k^2$ range over all of $\mathbb{Z}_k^2$ exactly once (Definition 2.14).

Using (1), it suffices to compute $\sum_J \widetilde{D_r(I,J)}$ for $r = 0, 1, 2, 3$.

Digits D_0, D_1 (within-block level). By Proposition 4.10,

$$D_0(I,J) = s\,i_0 + s^{-1}j_0, \qquad D_1(I,J) = s\,j_0 + s^{-1}i_0 \quad \text{in } \mathbb{Z}_k.$$

For fixed i_0, the map $j_0 \mapsto s\,i_0 + s^{-1}j_0$ is a bijection of $\mathbb{Z}_k$ (multiplication by $s^{-1} \neq 0$), and likewise $j_0 \mapsto s\,j_0 + s^{-1}i_0$ is a bijection [9]. Moreover, for each fixed j_0, there are exactly k choices of j_1. Therefore, by Lemma 5.1,

$$\sum_{J \in \mathbb{Z}_{k^2}} \widetilde{D_0(I,J)} = k \sum_{j_0 \in \mathbb{Z}_k} \widetilde{s\,i_0 + s^{-1}j_0} = k \cdot \frac{k(k-1)}{2} = \frac{k^2(k-1)}{2},$$

and similarly

$$\sum_{J\in\mathbb{Z}_{k^2}} \widetilde{D_1(I,J)} = \frac{k^2(k-1)}{2}.$$

Digits D_2, D_3 (block level). Again by Proposition 4.10,

$$D_2(I,J) = s\,i_1 + s^{-1}j_1, \qquad D_3(I,J) = s\,j_1 + s^{-1}i_1.$$

Now j_1 ranges over $\mathbb{Z}_k$ exactly k times as J ranges over $\mathbb{Z}_{k^2}$ (once for each j_0), and for fixed i_1 each of the maps $j_1 \mapsto s\,i_1 + s^{-1}j_1$ and $j_1 \mapsto s\,j_1 + s^{-1}i_1$ is bijective. Hence Lemma 5.1 gives

$$\sum_{J\in\mathbb{Z}_{k^2}} \widetilde{D_2(I,J)} = \frac{k^2(k-1)}{2}, \qquad \sum_{J\in\mathbb{Z}_{k^2}} \widetilde{D_3(I,J)} = \frac{k^2(k-1)}{2}.$$

Combining these four equalities with (1) yields

$$\begin{aligned}\sum_{J\in\mathbb{Z}_{k^2}} P_s(I,J) &= \frac{k^2(k-1)}{2}\,(1+k+k^2+k^3)\\ &= \frac{k^2(k-1)}{2}\cdot\frac{k^4-1}{k-1} = \frac{k^2(k^4-1)}{2}.\end{aligned}$$

□

Proposition 5.3 (Column sums). *For each fixed $J\in\mathbb{Z}_{k^2}$,*

$$\sum_{I\in\mathbb{Z}_{k^2}} P_s(I,J) = \frac{k^2(k^4-1)}{2}.$$

Proof. This is symmetric to Proposition 5.2 upon exchanging the roles of I and J. Formally, write $J \leftrightarrow (j_0, j_1)$ and let I range over $\mathbb{Z}_{k^2}$ with digits (i_0, i_1) ranging over $\mathbb{Z}_k^2$. Using Proposition 4.10, each digit $D_r(I,J)$ is an affine bijection in the varying digit (i_0 or i_1), and each such varying digit occurs with multiplicity k. Lemma 5.1 then gives the same total as in the row case. □

5.3. *Digit carry and borrow for toroidal diagonals*

To treat broken diagonals on $\mathbb{Z}_{k^2}^2$, we express the digit decomposition of $J = I \pm A$ in terms of the low digit carry/borrow. This is the only place where the toroidal indexing interacts nontrivially with the base-k digit decomposition.

Fix $A\in\mathbb{Z}_{k^2}$ and write $A \leftrightarrow (a_0, a_1)$ with $a_0, a_1 \in \mathbb{Z}_k$.

Definition 5.4 (Carry and borrow functions). For $t_0 \in \{0, 1, \dots, k-1\}$, define integers

$$\mathrm{car}_{a_0}(t_0) := \begin{cases} 1, & t_0 + \widetilde{a}_0 \geq k,\\ 0, & t_0 + \widetilde{a}_0 < k, \end{cases} \qquad \mathrm{bor}_{a_0}(t_0) := \begin{cases} 1, & t_0 > \widetilde{a}_0,\\ 0, & t_0 \leq \widetilde{a}_0. \end{cases}$$

Lemma 5.5 (Digit decomposition along slope $+1$ diagonals)**.** *Let $I \in \mathbb{Z}_{k^2}$ with $I \leftrightarrow (i_0, i_1)$, and put $J := I + A \in \mathbb{Z}_{k^2}$, where $A \leftrightarrow (a_0, a_1)$. Then $J \leftrightarrow (j_0, j_1)$ is given by*

$$j_0 \equiv i_0 + a_0 \pmod{k}, \qquad j_1 \equiv i_1 + a_1 + \mathrm{car}_{a_0}(\widetilde{i_0}) \pmod{k}.$$

Proof. Choose standard representatives $\widetilde{i_0}, \widetilde{i_1}, \widetilde{a_0}, \widetilde{a_1} \in \{0, 1, \dots, k-1\}$ and set $\widetilde{I} := \widetilde{i_0} + k\widetilde{i_1}$, $\widetilde{A} := \widetilde{a_0} + k\widetilde{a_1}$. Let $c := \mathrm{car}_{a_0}(\widetilde{i_0}) \in \{0, 1\}$. By definition of car_{a_0}, we have

$$\widetilde{i_0} + \widetilde{a_0} = (\widetilde{i_0} + \widetilde{a_0} - ck) + ck, \quad \text{with } 0 \le \widetilde{i_0} + \widetilde{a_0} - ck \le k - 1.$$

Hence

$$\widetilde{I} + \widetilde{A} = (\widetilde{i_0} + \widetilde{a_0} - ck) + k(\widetilde{i_1} + \widetilde{a_1} + c).$$

Reducing modulo k gives $j_0 \equiv i_0 + a_0 \pmod{k}$. Moreover, comparing the coefficients of k modulo k yields $j_1 \equiv i_1 + a_1 + c \equiv i_1 + a_1 + \mathrm{car}_{a_0}(\widetilde{i_0}) \pmod{k}$. □

Lemma 5.6 (Digit decomposition along slope -1 diagonals)**.** *Let $I \in \mathbb{Z}_{k^2}$ with $I \leftrightarrow (i_0, i_1)$, and put $J := -I + A \in \mathbb{Z}_{k^2}$, where $A \leftrightarrow (a_0, a_1)$. Then $J \leftrightarrow (j_0, j_1)$ is given by*

$$j_0 \equiv a_0 - i_0 \pmod{k}, \qquad j_1 \equiv a_1 - i_1 - \mathrm{bor}_{a_0}(\widetilde{i_0}) \pmod{k}.$$

Proof. Choose standard representatives $\widetilde{i_0}, \widetilde{i_1}, \widetilde{a_0}, \widetilde{a_1} \in \{0, 1, \dots, k-1\}$ and set $\widetilde{I} := \widetilde{i_0} + k\widetilde{i_1}$, $\widetilde{A} := \widetilde{a_0} + k\widetilde{a_1}$. Let $b := \mathrm{bor}_{a_0}(\widetilde{i_0}) \in \{0, 1\}$. By definition of bor_{a_0}, we have

$$\widetilde{a_0} - \widetilde{i_0} = (\widetilde{a_0} - \widetilde{i_0} + bk) - bk, \quad \text{with } 0 \le \widetilde{a_0} - \widetilde{i_0} + bk \le k - 1.$$

Hence

$$\widetilde{A} - \widetilde{I} = (\widetilde{a_0} - \widetilde{i_0} + bk) + k(\widetilde{a_1} - \widetilde{i_1} - b).$$

Reducing modulo k gives $j_0 \equiv a_0 - i_0 \pmod{k}$. Comparing the coefficients of k modulo k yields $j_1 \equiv a_1 - i_1 - b \equiv a_1 - i_1 - \mathrm{bor}_{a_0}(\widetilde{i_0}) \pmod{k}$. □

5.4. Broken diagonal sums

We now compute the sums of P_s along the broken diagonals of both slopes.

Proposition 5.7 (Broken diagonal sums, slope $+1$)**.** *For each $A \in \mathbb{Z}_{k^2}$,*

$$\sum_{I \in \mathbb{Z}_{k^2}} P_s(I,\, I + A) = \frac{k^2(k^4 - 1)}{2}.$$

Equivalently, for each $a \in \mathbb{Z}_{k^2}$ we have $\Delta_a^+(P_s) = \frac{k^2(k^4-1)}{2}$.

Proof. Fix $A \in \mathbb{Z}_{k^2}$ and write $A \leftrightarrow (a_0, a_1)$. Parameterize I by its digits $I \leftrightarrow (i_0, i_1) \in \mathbb{Z}_k^2$. Put $J := I + A$ and write $J \leftrightarrow (j_0, j_1)$. By Lemma 5.5,

$$j_0 \equiv i_0 + a_0, \qquad j_1 \equiv i_1 + a_1 + \mathrm{car}_{a_0}(\widetilde{i_0}) \pmod{k}.$$

Using (1), it suffices to show that for each $r = 0, 1, 2, 3$,

$$\sum_{I\in\mathbb{Z}_{k^2}} D_r(\widetilde{I,\, I+A}) = \frac{k^2(k-1)}{2}.$$

Digits D_0, D_1. By Proposition 4.10,

$$D_0(I,J) = M_s(i_0, j_0), \qquad D_1(I,J) = M_s^{\mathsf{T}}(i_0, j_0).$$

Along the slope $+1$ diagonal at offset a_0, we have $j_0 \equiv i_0 + a_0$. Hence i_1 plays no role, and each $i_0 \in \mathbb{Z}_k$ occurs with multiplicity k. Because s is admissible, M_s is toroidally diagonal-regular (Proposition 3.5), so the maps

$$i_0 \longmapsto M_s(i_0, i_0 + a_0), \qquad i_0 \longmapsto M_s^{\mathsf{T}}(i_0, i_0 + a_0),$$

are bijections of $\mathbb{Z}_k$. Therefore Lemma 5.1 gives

$$\sum_{I\in\mathbb{Z}_{k^2}} D_0(\widetilde{I, I+A}) = k \sum_{i_0\in\mathbb{Z}_k} M_s(\widetilde{i_0, i_0} + a_0) = k\cdot\frac{k(k-1)}{2} = \frac{k^2(k-1)}{2},$$

and similarly $\sum_I D_1(\widetilde{I, I+A}) = \frac{k^2(k-1)}{2}$.

Digits D_2, D_3. Again by Proposition 4.10,

$$D_2(I,J) = M_s(i_1, j_1), \qquad D_3(I,J) = M_s^{\mathsf{T}}(i_1, j_1).$$

For each fixed $i_0 \in \mathbb{Z}_k$, Lemma 5.5 shows that j_1 is of the form

$$j_1 \equiv i_1 + \Big(a_1 + \mathrm{car}_{a_0}(\widetilde{i_0})\Big) \pmod k.$$

Thus, for each fixed i_0, as i_1 ranges over $\mathbb{Z}_k$, the pair (i_1, j_1) runs along a slope $+1$ diagonal in $\mathbb{Z}_k^2$ with some offset $a_1 + \mathrm{car}_{a_0}(\widetilde{i_0})$. By diagonal-regularity of M_s (Proposition 3.5), the maps

$$i_1 \longmapsto M_s\left(i_1,\, i_1 + c\right), \qquad i_1 \longmapsto M_s^{\mathsf{T}}\left(i_1,\, i_1 + c\right),$$

are bijections for every $c \in \mathbb{Z}_k$. Hence, for each fixed i_0,

$$\sum_{i_1\in\mathbb{Z}_k} D_2(\widetilde{I, I+A}) = \frac{k(k-1)}{2}, \qquad \sum_{i_1\in\mathbb{Z}_k} D_3(\widetilde{I, I+A}) = \frac{k(k-1)}{2}.$$

Summing these equalities over the k choices of i_0 yields

$$\sum_{I\in\mathbb{Z}_{k^2}} D_2(\widetilde{I, I+A}) = \frac{k^2(k-1)}{2}, \qquad \sum_{I\in\mathbb{Z}_{k^2}} D_3(\widetilde{I, I+A}) = \frac{k^2(k-1)}{2}.$$

Combining the four digit sums with (1) gives

$$\sum_{I\in\mathbb{Z}_{k^2}} P_s(I, I+A) = \frac{k^2(k-1)}{2}\,(1+k+k^2+k^3) = \frac{k^2(k^4-1)}{2},$$

as required. □

Proposition 5.8 (Broken diagonal sums, slope -1)**.** *For each $A \in \mathbb{Z}_{k^2}$,*

$$\sum_{I\in\mathbb{Z}_{k^2}} P_s(I,\, -I+A) = \frac{k^2(k^4-1)}{2}.$$

Equivalently, for each $a \in \mathbb{Z}_{k^2}$ we have $\Delta_a^-(P_s) = \frac{k^2(k^4-1)}{2}$.

Proof. Fix $A \leftrightarrow (a_0, a_1)$ and parameterize $I \leftrightarrow (i_0, i_1) \in \mathbb{Z}_k^2$. Let $J := -I + A$ and write $J \leftrightarrow (j_0, j_1)$. By Lemma 5.6,

$$j_0 \equiv a_0 - i_0, \qquad j_1 \equiv a_1 - i_1 - \mathrm{bor}_{a_0}(\widetilde{i_0}) \pmod k.$$

As in Proposition 5.7, we compute digit sums.

Digits D_0, D_1. Here (i_0, j_0) runs along a slope -1 diagonal in $\mathbb{Z}_k^2$ with offset a_0: $j_0 \equiv -i_0 + a_0$. By diagonal-regularity of M_s (Proposition 3.5), the maps

$$i_0 \longmapsto M_s(i_0, -i_0 + a_0), \qquad i_0 \longmapsto M_s^{\mathsf{T}}(i_0, -i_0 + a_0),$$

are bijections of $\mathbb{Z}_k$. Each i_0 occurs with multiplicity k (varying i_1), so Lemma 5.1 yields

$$\sum_{I\in\mathbb{Z}_{k^2}} D_0(\widetilde{I, -I+A}) = \frac{k^2(k-1)}{2}, \qquad \sum_{I\in\mathbb{Z}_{k^2}} D_1(\widetilde{I, -I+A}) = \frac{k^2(k-1)}{2}.$$

Digits D_2, D_3. For each fixed i_0, Lemma 5.6 shows that j_1 is of the form

$$j_1 \equiv -i_1 + \Big(a_1 - \mathrm{bor}_{a_0}(\widetilde{i_0})\Big) \pmod k.$$

Thus (i_1, j_1) runs along a slope -1 diagonal in $\mathbb{Z}_k^2$ (with an offset depending on i_0). By diagonal-regularity of M_s, along any such diagonal the maps $i_1 \mapsto M_s(i_1, -i_1 + c)$ and $i_1 \mapsto M_s^{\mathsf{T}}(i_1, -i_1 + c)$ are bijections. Hence for each fixed i_0 the sums over i_1 equal $\frac{k(k-1)}{2}$, and summing over i_0 gives

$$\sum_{I\in\mathbb{Z}_{k^2}} D_2(\widetilde{I, -I+A}) = \frac{k^2(k-1)}{2}, \qquad \sum_{I\in\mathbb{Z}_{k^2}} D_3(\widetilde{I, -I+A}) = \frac{k^2(k-1)}{2}.$$

Substituting into (1) yields $\sum_I P_s(I, -I+A) = \frac{k^2(k^4-1)}{2}$, as required. □

5.5. *Conclusion: P_s is pandiagonal magic*

Theorem 5.9 (Pandiagonality of the encoded square)**.** *Let $k \geq 7$ be prime and let $s \in \mathbb{Z}_k^\times$ satisfy $s^2 \not\equiv \pm 1 \pmod k$. Then the encoded square $P_s : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}$ from Construction 4.7 is* a normal pandiagonal magic square *of order k^2 with entry set $\{0, 1, \ldots, k^4 - 1\}$. Moreover, every row sum, column sum, and broken diagonal sum (both slopes) equals*

$$\mu = \frac{k^2(k^4-1)}{2}.$$

Proof. Normality (entry set $\{0, 1, \ldots, k^4 - 1\}$ with no repetition) is Proposition 4.8. Row sums are constant by Proposition 5.2, and column sums are constant by Proposition 5.3. Broken diagonal sums of slope $+1$ and -1 are constant by Propositions 5.7 and 5.8. Thus P_s is pandiagonal magic in the sense of Definition 2.2. Finally, since P_s is normal of order $m = k^2$, the common sum must equal the standard magic constant $m(m^2 - 1)/2 = \frac{k^2(k^4-1)}{2}$ by Proposition 2.3. □

Remark 5.10 (Where orthogonality and diagonal-regularity enter)**.** Orthogonality with the transpose (Section 4) is used only to guarantee normality (bijectivity of digit tuples), while diagonal-regularity of the kernel (Proposition 3.5) is the mechanism ensuring that each digit array restricts to a permutation along the relevant toroidal diagonals. This separation clarifies the logic in the diabolic/Nasik setting initiated in [6, 14].

6. The compound property via block sums

In this section we prove that the pandiagonal magic square P_s constructed in Section 4 is in fact *compound pandiagonal magic* in the sense of Definition 2.18. Compound constructions of magic squares (often via Latin-square superpositions or digit concatenations) appear in the classical literature and modern treatments; see, for example, [1, 10]. Our contribution here is to show that, for the present closed-form P_s, the induced $k \times k$ *block-sum array* is itself pandiagonal magic, and to compute it explicitly.

Throughout, $k \geq 7$ is prime and $s \in \mathbb{Z}_k^\times$ satisfies

$$s^2 \not\equiv \pm 1 \pmod{k},$$

so that P_s is a normal pandiagonal magic square of order k^2 by Theorem 5.9.

6.1. Block notation and reduction to digit sums

Recall the index-digit decomposition $I \leftrightarrow (i_0, i_1)$ and $J \leftrightarrow (j_0, j_1)$ from Definition 2.14. The block index of a cell $(I, J) \in \mathbb{Z}_{k^2}^2$ is $(i_1, j_1) \in \mathbb{Z}_k^2$, and the within-block position is $(i_0, j_0) \in \mathbb{Z}_k^2$ (Remark 2.15).

Remark 6.1 (Block and block sum)**.** Let $u, v \in \mathbb{Z}_k$. Define the (u, v)-*block* of $\mathbb{Z}_{k^2}^2$ by

$$B_{u,v} := \{(I, J) \in \mathbb{Z}_{k^2}^2 \mid I \leftrightarrow (i_0, u),\ J \leftrightarrow (j_0, v) \text{ for some } (i_0, j_0) \in \mathbb{Z}_k^2\}.$$

For an array $A : \mathbb{Z}_{k^2}^2 \to \mathbb{Z}$, define the *block sum*

$$\Sigma_{u,v}(A) := \sum_{(I,J) \in B_{u,v}} A(I, J).$$

We write $\Sigma(A) : \mathbb{Z}_k^2 \to \mathbb{Z}$ for the induced $k \times k$ array $\Sigma(A)(u, v) := \Sigma_{u,v}(A)$.

This agrees with Definition 2.18, included here for local reference.

Our starting point is to insert the digit expansion (1) of P_s and separate sums over within-block digits (i_0, j_0) from sums over block digits (u, v).

6.2. *Explicit formula for block sums*

We emphasize that in the digit expansion of P_s (Construction 4.7), the digits D_0, D_1 vary within each block, whereas D_2, D_3 depend only on the block indices (u, v). This separation is standard in compound constructions; see, e.g., [14, 10].

Proposition 6.2 (Within-block digit totals). *Fix $(u, v) \in \mathbb{Z}_k^2$ and consider the block $B_{u,v}$. Then, for the encoded square P_s,*

$$\sum_{(I,J)\in B_{u,v}} \widetilde{D_0(I,J)} \;=\; \sum_{(I,J)\in B_{u,v}} \widetilde{D_1(I,J)} \;=\; \frac{k^2(k-1)}{2}.$$

Proof. Inside the fixed block $B_{u,v}$ we have $i_1 = u$ and $j_1 = v$ fixed, while (i_0, j_0) ranges over $\mathbb{Z}_k^2$ exactly once. By Proposition 4.10 (the closed form for P_s), we have

$$D_0 = si_0 + s^{-1}j_0, \qquad D_1 = sj_0 + s^{-1}i_0 \quad \text{in } \mathbb{Z}_k.$$

Thus as (i_0, j_0) runs over $\mathbb{Z}_k^2$, each of D_0 and D_1 runs over $\mathbb{Z}_k$ exactly k times: for each fixed i_0, the map $j_0 \mapsto si_0 + s^{-1}j_0$ is bijective (since $s^{-1} \in \mathbb{Z}_k^\times$), and similarly for D_1. Therefore Lemma 5.1 yields

$$\sum_{(I,J)\in B_{u,v}} \widetilde{D_0(I,J)} = k\sum_{x=0}^{k-1} x = \frac{k^2(k-1)}{2},$$

and the same computation applies to D_1. □

Lemma 6.3 (Block-level digit totals). *Fix $(u, v) \in \mathbb{Z}_k^2$ and consider the block $B_{u,v}$. Then within $B_{u,v}$ the digits D_2, D_3 are constant and satisfy*

$$D_2(I,J) = su + s^{-1}v, \qquad D_3(I,J) = sv + s^{-1}u \quad \text{in } \mathbb{Z}_k \qquad ((I,J) \in B_{u,v}),$$

hence

$$\sum_{(I,J)\in B_{u,v}} \widetilde{D_2(I,J)} = k^2\, \widetilde{su + s^{-1}v}, \qquad \sum_{(I,J)\in B_{u,v}} \widetilde{D_3(I,J)} = k^2\, \widetilde{sv + s^{-1}u}.$$

Proof. This is immediate from Proposition 4.10: the digits D_2, D_3 depend only on $(i_1, j_1) = (u, v)$ and are independent of the within-block digits (i_0, j_0). Since $|B_{u,v}| = k^2$, the asserted sums follow. □

Proposition 6.4 (Closed form for the block-sum array). *Let $(u, v) \in \mathbb{Z}_k^2$. Then the block sum of P_s over $B_{u,v}$ equals*

$$\Sigma_{u,v}(P_s) = \frac{k^2(k-1)}{2}(1+k) \;+\; k^2\left(\widetilde{su + s^{-1}v}\right)k^2 \;+\; k^2\left(\widetilde{sv + s^{-1}u}\right)k^3, \tag{2}$$

i.e.

$$\Sigma_{u,v}(P_s) = \frac{k^2(k-1)}{2}(1+k) \;+\; k^4\, \widetilde{su + s^{-1}v} \;+\; k^5\, \widetilde{sv + s^{-1}u}.$$

Proof. Fix (u, v) and sum the digit expansion (Construction 4.7) over the block $B_{u,v}$:

$$\begin{aligned}\Sigma_{u,v}(P_s) = \sum_{(I,J)\in B_{u,v}} \widetilde{D_0(I,J)} + k \sum_{(I,J)\in B_{u,v}} \widetilde{D_1(I,J)} +\\ k^2 \sum_{(I,J)\in B_{u,v}} \widetilde{D_2(I,J)} + k^3 \sum_{(I,J)\in B_{u,v}} \widetilde{D_3(I,J)}.\end{aligned}$$

By Proposition 6.2 the first two sums equal $\frac{k^2(k-1)}{2}$, and by Lemma 6.3 the last two sums equal $k^2\widetilde{su + s^{-1}v}$ and $k^2\widetilde{sv + s^{-1}u}$, respectively. Substituting gives (2). □

Remark 6.5 (Normalization of the block-sum array)**.** The factor k^2 in the last two terms of (2) shows that the block-sum array is, up to an additive constant and a scaling, a base-k superposition of the two block-level digits

$$D_2(u, v) = M_s(u, v), \qquad D_3(u, v) = M_s^{\mathsf{T}}(u, v),$$

so the compound property is inherited from the same kernel structure; compare [14, 10].

6.3. *Pandiagonality of the block-sum array*

Define the *reduced block-sum array* by subtracting the constant within-block contribution and dividing out the common factor k^4.

Definition 6.6 (Reduced block-sum array)**.** Define $Q_s : \mathbb{Z}_k^2 \to \mathbb{Z}$ by

$$Q_s(u, v) := \frac{1}{k^4}\left(\Sigma_{u,v}(P_s) - \frac{k^2(k-1)}{2}(1+k)\right).$$

Equivalently, by Proposition 6.4,

$$Q_s(u, v) = \widetilde{M_s(u, v)} + k\,\widetilde{M_s^{\mathsf{T}}(u, v)}.$$

Remark 6.7. The array Q_s is the base-k encoding of the ordered pair $\left(M_s, M_s^{\mathsf{T}}\right)$. This is the standard "superposition" mechanism in the Latin-square literature [5, 4].

Proposition 6.8 (Row and column sums of Q_s)**.** *For each fixed $u \in \mathbb{Z}_k$,*

$$\sum_{v\in\mathbb{Z}_k} Q_s(u, v) = \sum_{v\in\mathbb{Z}_k} \left(\widetilde{M_s(u, v)} + k\,\widetilde{M_s^{\mathsf{T}}(u, v)}\right) = \frac{k(k-1)}{2}\,(1+k),$$

and similarly for each fixed $v \in \mathbb{Z}_k$,

$$\sum_{u\in\mathbb{Z}_k} Q_s(u, v) = \frac{k(k-1)}{2}\,(1+k).$$

Proof. Fix u. As v ranges over $\mathbb{Z}_k$, the map $v \mapsto M_s(u,v) = s\,u + s^{-1}v$ is a bijection of $\mathbb{Z}_k$ (Proposition 3.3), hence $\sum_v \widetilde{M_s(u,v)} = \frac{k(k-1)}{2}$ by Lemma 5.1. Also $v \mapsto M_s^{\mathsf{T}}(u,v) = M_s(v,u) = s\,v + s^{-1}u$ is bijective in v, hence $\sum_v \widetilde{M_s^{\mathsf{T}}(u,v)} = \frac{k(k-1)}{2}$. Thus

$$\sum_v Q_s(u,v) = \frac{k(k-1)}{2} + k \cdot \frac{k(k-1)}{2} = \frac{k(k-1)}{2}(1+k).$$

The column-sum identity is symmetric. □

Proposition 6.9 (Broken diagonal sums of Q_s)**.** *For each $a \in \mathbb{Z}_k$,*

$$\sum_{t\in\mathbb{Z}_k} Q_s(t,t+a) = \sum_{t\in\mathbb{Z}_k} Q_s(t,-t+a) = \frac{k(k-1)}{2}(1+k).$$

Equivalently, Q_s is a pandiagonal magic square of order k.

Proof. Fix $a \in \mathbb{Z}_k$. Along the slope $+1$ diagonal, $v = t+a$. By Proposition 3.5 (diagonal-regularity), the maps $t \mapsto M_s(t,t+a)$ and $t \mapsto M_s^{\mathsf{T}}(t,t+a)$ are bijections of $\mathbb{Z}_k$. Hence Lemma 5.1 gives

$$\sum_t \widetilde{M_s(t,t+a)} = \frac{k(k-1)}{2}, \qquad \sum_t \widetilde{M_s^{\mathsf{T}}(t,t+a)} = \frac{k(k-1)}{2},$$

and therefore

$$\sum_t Q_s(t,t+a) = \frac{k(k-1)}{2} + k \cdot \frac{k(k-1)}{2} = \frac{k(k-1)}{2}(1+k).$$

The slope -1 case is identical, using diagonal-regularity along $v = -t+a$. Thus Q_s is pandiagonal magic by Definition 2.2. □

Corollary 6.10 (Pandiagonality of the block-sum array)**.** *The block-sum array $\Sigma(P_s)$ is pandiagonal magic of order k.*

Proof. By Definition 6.6,

$$\Sigma_{u,v}(P_s) = \frac{k^2(k-1)}{2}(1+k) + k^4\,Q_s(u,v).$$

Adding a constant to all entries and multiplying by a positive scalar preserves the property that all row/column/broken-diagonal sums are constant (Definition 2.2). Since Q_s is pandiagonal magic by Proposition 6.9, it follows that $\Sigma(P_s)$ is pandiagonal magic as well. □

6.4. Compound pandiagonal magic squares

Theorem 6.11 (Compound property)**.** *Let $k \geq 7$ be prime and let $s \in \mathbb{Z}_k^\times$ satisfy $s^2 \not\equiv \pm 1 \pmod{k}$. Then the encoded square P_s is a* compound pandiagonal normal magic square *of order k^2 in the sense of Definition 2.18.*

Proof. By Theorem 5.9, P_s is a normal pandiagonal magic square of order k^2. By Corollary 6.10, the block-sum array $\Sigma(P_s)$ is a pandiagonal magic square of order k. These two statements are exactly the conditions in Definition 2.18. □

Remark 6.12 (Logical structure)**.** The compound property splits cleanly into: (i) within-block digits (D_0, D_1) contribute only a blockwise constant to $\Sigma(P_s)$, and (ii) block-level digits (D_2, D_3) reproduce, after scaling, the same base-k superposition mechanism already used at the $k^2 \times k^2$ level. This explains why the construction remains closed-form and why no search is required at either level.

7. Examples, Parameter Choices, and Verification

This section records practical choices of the MIS parameter s, gives a worked example, and summarizes straightforward verification steps. The construction itself is fully explicit (Sections 3–6); the present section is intended for readability and reproducibility.

7.1. Admissible MIS parameters

Recall that the construction requires a prime $k \geq 7$ and a parameter $s \in \mathbb{Z}_k^\times$ satisfying

$$s^2 \not\equiv \pm 1 \pmod{k}. \tag{3}$$

By Corollary 3.8, this single condition simultaneously ensures: (i) M_s is a Latin square, (ii) M_s is toroidally diagonal-regular, and (iii) M_s is orthogonal to M_s^T. The role of (3) is thus exactly the standard nondegeneracy needed for linear Latin squares and their orthogonality properties [7, 5, 4].

Proposition 7.1 (Counting admissible parameters)**.** *Let k be an odd prime, and recall the set $S_k \subseteq \mathbb{Z}_k^\times$ defined in Remark 3.9. Then*

$$|S_k| = (k-1) - 2 - \nu_k,$$

where $\nu_k \in \{0, 2\}$ is the number of solutions of $x^2 \equiv -1 \pmod{k}$. More explicitly,

$$|S_k| = \begin{cases} k-3, & k \equiv 3 \pmod{4}, \\ k-5, & k \equiv 1 \pmod{4}. \end{cases}$$

Proof. There are exactly two solutions of $x^2 \equiv 1 \pmod{k}$, namely $x \equiv \pm 1$. Let ν_k be the number of solutions of $x^2 \equiv -1 \pmod{k}$. Then S_k is obtained from $\mathbb{Z}_k^\times$ by removing the two elements with square 1 and the ν_k elements with square -1, giving $|S_k| = (k-1)-2-\nu_k$.

Finally, the classical criterion states that -1 is a quadratic residue modulo an odd prime k if and only if $k \equiv 1 \pmod 4$, in which case there are exactly two square roots of -1 in $\mathbb{Z}_k$; otherwise there are none (see, e.g., [9, § 3.5]). This yields the explicit cases. □

Remark 7.2 (Smallest admissible prime)**.** For $k = 5$, every nonzero square is ± 1 modulo 5, hence $S_5 = \varnothing$. Thus the smallest prime for which admissible parameters exist is $k = 7$.

7.2. *A worked example: $k = 7$ and $s = 2$*

Let $k = 7$ and choose $s = 2 \in \mathbb{Z}_7^\times$. Then $s^{-1} = 4$ in $\mathbb{Z}_7$. Since $s^2 = 4 \not\equiv \pm 1 \pmod 7$, the admissibility condition (3) holds, and Theorems 5.9 and 6.11 apply.

Example 7.3 (Closed form for the entry function)**.** Write indices $I, J \in \mathbb{Z}_{49}$ uniquely as

$$I \leftrightarrow (i_0, i_1), \qquad J \leftrightarrow (j_0, j_1), \qquad (i_0, i_1, j_0, j_1 \in \mathbb{Z}_7),$$

meaning $I \equiv i_0 + 7i_1$ and $J \equiv j_0 + 7j_1$. Then Proposition 4.10 gives the digits

$$D_0 = 2i_0 + 4j_0, \quad D_1 = 2j_0 + 4i_0, \quad D_2 = 2i_1 + 4j_1, \quad D_3 = 2j_1 + 4i_1 \quad \text{in } \mathbb{Z}_7,$$

and the entry is

$$P_2(I, J) = \widetilde{D_0} + 7\widetilde{D_1} + 49\widetilde{D_2} + 343\widetilde{D_3} \in \{0, 1, \dots, 2400\}.$$

For instance:

(i) $(I, J) = (0, 0)$ has $(i_0, i_1, j_0, j_1) = (0, 0, 0, 0)$, hence $P_2(0, 0) = 0$.

(i) $(I, J) = (0, 1)$ has $(0, 0, 1, 0)$, hence $(D_0, D_1, D_2, D_3) = (4, 2, 0, 0)$ and $P_2(0, 1) = 4 + 7 \cdot 2 = 18$.

(i) $(I, J) = (1, 0)$ has $(1, 0, 0, 0)$, hence $(D_0, D_1, D_2, D_3) = (2, 4, 0, 0)$ and $P_2(1, 0) = 2 + 7 \cdot 4 = 30$.

Remark 7.4 (Magic constants)**.** For $k = 7$, the order is $k^2 = 49$ and the entry set is $\{0, 1, \dots, k^4 - 1\} = \{0, 1, \dots, 2400\}$. By Theorem 5.9, every row/column/broken diagonal sum equals

$$\mu = \frac{k^2(k^4 - 1)}{2} = \frac{49 \cdot 2400}{2} = 58800.$$

Moreover, the block-sum array $\Sigma(P_s)$ is a 7×7 pandiagonal magic square. Each of its row sums equals the sum of the 7 row sums of P_s in the corresponding block-row, hence equals $7\mu = 411600$.

7.3. *Further admissible choices*

The admissibility test (3) is trivial to apply: compute $s^2 \bmod k$ and exclude the cases $s^2 \equiv 1$ and $s^2 \equiv -1$. For example:

Example 7.5 (Some admissible parameters)**.** (i) $k = 7$: admissible s are $\{2, 3, 4, 5\}$ (since $s = \pm 1$ are excluded and $-1 \equiv 6$ has no square root modulo 7).

(ii) $k = 11$: admissible s include $s = 2, 3, 4, 5, 6, 7, 8, 9$ except $s = \pm 1$ and $s^2 \equiv -1 \equiv 10$ (which has no solution because $11 \equiv 3 \pmod 4$).

(iii) $k = 13$: since $13 \equiv 1 \pmod 4$, there are two solutions of $s^2 \equiv -1 \pmod{13}$ and these must also be excluded; thus $|S_{13}|= 8$ by Proposition 7.1.

7.4. *Verification checklist (computational and conceptual)*

Although the main results have been proved in Sections 4–6, it is often desirable (for refereeing or for implementation) to have a clear verification checklist. The following items can be checked directly from the closed form in Proposition 4.10 using any CAS, e.g. Magma [3].

Remark 7.6 (Finite verification steps)**.** Fix a prime k and $s \in \mathbb{Z}_k^\times$ satisfying (3). Define P_s by Construction 4.7. Then each of the following provides an independent sanity check of correctness:

(1) *Normality:* verify that the map $(I, J) \mapsto P_s(I, J)$ is injective on $\mathbb{Z}_{k^2}^2$ (hence bijective onto $\{0, \dots, k^4 - 1\}$), equivalently verify digit-tuple bijectivity (Proposition 4.8).

(2) *Pandiagonality:* verify constancy of the row sums $R_I(P_s)$ and column sums $C_J(P_s)$ (Propositions 5.2, 5.3), and the broken diagonal sums (Propositions 5.7, 5.8).

(3) *Compound property:* compute block sums $\Sigma_{u,v}(P_s)$ and verify that the $k \times k$ array $\Sigma(P_s)$ is pandiagonal magic (Corollary 6.10).

Remark 7.7 (Complexity and random access)**.** The closed form in Proposition 4.10 evaluates a single entry $P_s(I, J)$ using a constant number of modular multiplications in $\mathbb{Z}_k$ and a base-k encoding. Thus the construction supports *random access* to entries without generating the whole $k^2 \times k^2$ array, which is an important algorithmic advantage emphasized in the Introduction.

7.5. *Algorithmic summary and tested cases*

Construction 7.8 (Algorithmic generation of P_s)**.** Input: a prime k and $s \in \mathbb{Z}_k^\times$ satisfying $s^2 \not\equiv \pm 1 \pmod k$.

(a) (Kernel digits) For $(i, j) \in \mathbb{Z}_k^2$, define

$$M_s(i, j) := si + s^{-1}j \in \mathbb{Z}_k, \qquad M_s^{\mathsf{T}}(i, j) := M_s(j, i).$$

(b) (Index splitting) For $I, J \in \mathbb{Z}_{k^2}$, write uniquely

$$I \equiv i_0 + ki_1, \quad J \equiv j_0 + kj_1 \qquad (i_0, i_1, j_0, j_1 \in \mathbb{Z}_k).$$

(c) (Four digits) Set

$$D_0 := M_s(i_0, j_0), \; D_1 := M_s^{\mathsf{T}}(i_0, j_0), \; D_2 := M_s(i_1, j_1), \; D_3 := M_s^{\mathsf{T}}(i_1, j_1).$$

(d) (Base-k encoding) Output

$$P_s(I, J) := D_0 + kD_1 + k^2D_2 + k^3D_3 \in \{0, 1, \dots, k^4 - 1\} \subset \mathbb{Z}.$$

The sample computational checks (sanity verification) is given in Table 2.

Table 2. Sample computational checks (sanity verification)

prime k	admissible s (examples)	checked items	result
7	$2, 3, 4, 5$	(1)–(3) in Remark 7.6	pass
11	$2, 3, 4, 5, 6, 7, 8, 9$	(1)–(3) in Remark 7.6	pass
13	any $s \in S_{13}$	(1)–(3) in Remark 7.6	pass

Example 7.9 (A concrete $k \times k$ block excerpt ($k = 7$, $s = 2$))**.** Let $k = 7$ and $s = 2 \in \mathbb{Z}_7^\times$, so $s^{-1} = 4$. Consider the block $(i_1, j_1) = (0, 0)$ in the $k^2 \times k^2$ square P_s. For indices $I \leftrightarrow (i_0, 0)$ and $J \leftrightarrow (j_0, 0)$ we have $D_2 = D_3 = 0$, hence

$$P_s(I, J) = \widetilde{D_0} + 7\widetilde{D_1}, \qquad D_0 \equiv 2i_0 + 4j_0, \quad D_1 \equiv 2j_0 + 4i_0 \pmod 7.$$

Thus the $(0, 0)$-block of P_s (rows indexed by i_0, columns by j_0) is the following 7×7 array with entries in $\{0, 1, \dots, 48\}$:

	0	1	2	3	4	5	6
0	0	18	29	47	9	27	38
1	30	48	10	21	39	1	19
2	11	22	40	2	20	31	42
3	41	3	14	32	43	12	23
4	15	33	44	13	24	35	4
5	45	7	25	36	5	16	34
6	26	37	6	17	28	46	8

This excerpt illustrates how the within-block digits (D_0, D_1) already encode a normal 7×7 pattern; the remaining digits (D_2, D_3) shift/stack such blocks across the 7×7 block grid according to Construction 4.7.

8. Discussion and Further Directions

This final section clarifies the conceptual status of the MIS kernel in the Latin-square literature, records degrees of freedom beyond the specific kernel–transpose choice, and lists natural extensions and open directions. Standard background on Latin squares, orthogonality, and isotopisms can be found in [5, 4], and early algebraic treatments of pandiagonal (diabolic/Nasik) conditions appear in [6, 14].

8.1. The MIS kernel as a classical linear Latin square

We emphasized in the Introduction that the novelty of the present work is not the discovery of a new Latin-square object, but rather the closed-form, search-free integration into a compound pandiagonal magic-square construction. The following proposition makes the "classical" status of the MIS kernel precise.

Definition 8.1 (Isotopism and isotopy)**.** Let $L, L' : \mathbb{Z}_k^2 \to \mathbb{Z}_k$ be Latin squares. An *isotopism* from L to L' is a triple of permutations $(\alpha, \beta, \gamma) \in \mathrm{Sym}(\mathbb{Z}_k)^3$ such that

$$L'(\alpha(i), \beta(j)) = \gamma\,(L(i,j)) \qquad (\forall\, i, j \in \mathbb{Z}_k).$$

If such an isotopism exists, we say that L and L' are *isotopic*.

Isotopy is a standard equivalence relation in Latin-square theory [5, 4].

Proposition 8.2 (Linear Latin squares are isotopic to addition tables)**.** *Let k be prime and let $a, b \in \mathbb{Z}_k^\times$. Then the linear Latin square $L_{a,b}(i,j) = ai + bj$ is isotopic to the group table*

$$T(i,j) := i + j, \qquad (i, j \in \mathbb{Z}_k),$$

of the cyclic group $(\mathbb{Z}_k, +)$.

Proof. Define permutations $\alpha, \beta, \gamma \in \mathrm{Sym}(\mathbb{Z}_k)$ by

$$\alpha(i) := a^{-1}i, \qquad \beta(j) := b^{-1}j, \qquad \gamma(x) := x.$$

Then for all $i, j \in \mathbb{Z}_k$,

$$T(\alpha(i), \beta(j)) = \alpha(i) + \beta(j) = a^{-1}i + b^{-1}j.$$

Applying the permutation $\gamma_a : x \mapsto ab\,x$ (also a permutation of $\mathbb{Z}_k$) gives

$$\gamma_a\,(T(\alpha(i), \beta(j))) = ab(a^{-1}i + b^{-1}j) = bi + aj.$$

Composing with the transpose isotopism $(i, j) \mapsto (j, i)$ if needed, we obtain an isotopism to $L_{a,b}(i,j) = ai + bj$. Equivalently, one may choose (α, β, γ) directly to solve $\gamma(i + j) = ai + bj$ by scaling symbols and coordinates; this is standard for group-based linear Latin squares [5]. □

Corollary 8.3 (MIS kernel is classical up to isotopy)**.** *For every $s \in \mathbb{Z}_k^\times$, the MIS kernel $M_s(i,j) = si + s^{-1}j$ (Definition 3.1) is isotopic to the addition table of $(\mathbb{Z}_k, +)$.*

Proof. Apply Proposition 8.2 with $(a, b) = (s, s^{-1})$. □

Remark 8.4 (Interpretation)**.** Corollary 8.3 formalizes the point used in the novelty discussion: the MIS kernel is a member of the well-understood class of linear Latin squares. The present contribution is that a particular inverse-coupled parameterization $(a, b) = (s, s^{-1})$, together with a two-level base-k encoding, yields a closed-form construction of *compound pandiagonal* normal magic squares of order k^2 (Theorem 6.11), without any search step.

8.2. *Orthogonality and degrees of freedom*

The construction used a specific orthogonal pair (M_s, M_s^{T}). From the Latin-square viewpoint, many other orthogonal pairs exist, and linear families over $\mathbb{Z}_k$ provide complete sets of mutually orthogonal Latin squares (MOLS) for prime k [5, 4].

Definition 8.5 (Mutually orthogonal Latin squares)**.** A set $\{L_t : \mathbb{Z}_k^2 \to \mathbb{Z}_k\}_{t\in T}$ of Latin squares is called a set of *mutually orthogonal Latin squares* (MOLS) if L_t and $L_{t'}$ are orthogonal for all distinct $t, t' \in T$.

Proposition 8.6 (A complete linear family for prime k)**.** *Let k be prime and, for each $t \in \mathbb{Z}_k^{\times}$, define*

$$L_t(i,j) := i + tj \qquad (i,j \in \mathbb{Z}_k).$$

Then $\{L_t\}_{t\in\mathbb{Z}_k^{\times}}$ is a set of $k-1$ MOLS of order k.

Proof. Each L_t is Latin since $t \neq 0$ (Definition 2.4). For distinct $t, t' \in \mathbb{Z}_k^{\times}$, apply Proposition 2.10 to the pair $L_t = L_{1,t}$ and $L_{t'} = L_{1,t'}$:

$$\det\begin{pmatrix} 1 & t \\ 1 & t' \end{pmatrix} = t' - t \neq 0 \quad \text{in } \mathbb{Z}_k.$$

Hence L_t and $L_{t'}$ are orthogonal. □

Remark 8.7 (Relation to the MIS choice)**.** The MIS pair (M_s, M_s^{T}) is a very specific orthogonal pair inside the linear family: orthogonality reduces to $s^2 \not\equiv \pm 1$ (Proposition 3.7), which is a particularly simple congruence test. Other choices of orthogonal pairs may lead to further explicit constructions, but preserving *toroidal diagonal-regularity* (needed for pandiagonality) imposes additional constraints (Proposition 3.5).

8.3. *Higher-level encodings and multi-compound variants*

The present paper treats the first nontrivial compound level: order k^2 with entries $\{0, 1, \ldots, k^4 - 1\}$, obtained by a two-level digit system. A natural extension is to iterate the digit mechanism to obtain order k^m objects for $m \geq 3$.

Definition 8.8 (m-level digit decomposition)**.** Let $m \geq 1$. For $I \in \mathbb{Z}_{k^m}$, define digits $(i_0, \ldots, i_{m-1}) \in \mathbb{Z}_k^m$ by the unique congruence

$$I \equiv i_0 + ki_1 + \cdots + k^{m-1} i_{m-1} \pmod{k^m}, \qquad i_r \in \{0, 1, \ldots, k-1\}.$$

We write $I \leftrightarrow (i_0, \ldots, i_{m-1})$.

Construction 8.9 (Iterated orthogonal digit superposition)**.** Fix $s \in \mathbb{Z}_k^{\times}$. For $(I, J) \in \mathbb{Z}_{k^m}^2$ with $I \leftrightarrow (i_0, \ldots, i_{m-1})$ and $J \leftrightarrow (j_0, \ldots, j_{m-1})$, define $2m$ digit functions $E_0, \ldots, E_{2m-1} : \mathbb{Z}_{k^m}^2 \to \mathbb{Z}_k$ by

$$(E_{2r}(I,J), E_{2r+1}(I,J)) := \Phi_s(i_r, j_r) \qquad (0 \leq r \leq m-1),$$

where Φ_s is the kernel pair map (Definition 4.1). Then define the base-k encoding

$$P_s^{(m)}(I,J) := \mathrm{enc}_k\left(E_0(I,J), E_1(I,J), \dots, E_{2m-1}(I,J)\right) = \sum_{r=0}^{2m-1} k^r\, \widetilde{E_r(I,J)}.$$

Remark 8.10 (What is immediate, what is not)**.** If Φ_s is bijective (equivalently $s^2 \not\equiv \pm 1$), then the same product-bijection argument as in Proposition 4.8 shows that $P_s^{(m)}$ is *normal*: it is a bijection from $\mathbb{Z}_{k^m}^2$ to $\{0,1,\dots,k^{2m}-1\}$. Row and column sums can also be handled digitwise exactly as in Propositions 5.2 and 5.3. However, for pandiagonal (broken diagonal) sums one must control carries/borrows across *all* digit levels, generalizing Lemmas 5.5 and 5.6. We leave a full treatment of this multi-level carry analysis to future work.

Problem 8.11 (Higher-level pandiagonality and multi-compound structure)**.** *Assume k is prime and $s \in \mathbb{Z}_k^\times$ satisfies $s^2 \not\equiv \pm 1$.*

(i) *Determine for which $m \geq 3$ the iterated encoding $P_s^{(m)}$ of Construction 8.9 is pandiagonal magic of order k^m.*

(ii) *Formulate and prove an appropriate notion of* multi-compound *property (e.g. pandiagonality of induced block-sum arrays at each intermediate scale k^r, $1 \leq r < m$), and decide whether $P_s^{(m)}$ satisfies it.*

8.4. Beyond primes and further constraints

The present article focuses on prime k so that $\mathbb{Z}_k$ is a field and the arithmetic and digit representatives are canonical. Linear Latin-square orthogonality and MOLS theory extends to prime powers via finite fields [9, 5, 4], but *normality with consecutive integer entries* is most naturally phrased in the prime setting due to the base-k encoding into $\{0,1,\dots,k^t-1\}$.

Problem 8.12 (Composite moduli and non-field effects)**.** *Develop an analogue of the MIS construction for composite moduli n where $\mathbb{Z}_n$ is not a field. In particular, determine whether there exist explicit parameter families yielding:*

(i) *Latin-square kernels over $\mathbb{Z}_n$ with suitable toroidal diagonal-regularity;*

(ii) *orthogonality sufficient to guarantee normality of an encoding map;*

(iii) *pandiagonality and compound pandiagonality at order n^2.*

Any such extension must address the failure of invertibility for zero divisors and the resulting breakdown of the determinant criterion in Proposition 2.10.

Remark 8.13 (Additional magic constraints)**.** Pandiagonality is only one layer in the hierarchy of "strong" magic conditions. Classical and modern literature also considers refinements such as *most-perfect* (and related panmagic variants), which typically impose additional complementary sum rules and stronger regularity across subsquares, beyond the broken-diagonal constraints; see, e.g., [11, 1]. Another direction is to require higher-moment constraints (bimagic, trimagic, etc.), where not only the entries but also their powers satisfy prescribed line-sum conditions.

From the viewpoint of the present paper, it is natural to ask which of these stronger properties can be compatible with a fully explicit digit-superposition construction with random-access evaluation. Concretely, one may test whether such constraints can be enforced by simple arithmetic restrictions on the kernel parameters, or whether they necessarily require non-linear modifications (or additional digit layers) beyond the linear MIS framework.

8.5. Summary of the novelty claim

We close by reiterating, in the precise language developed above, how the work sits relative to existing theory.

Remark 8.14 (Kernel vs. construction)**.** (1) *Kernel level (known).* The MIS kernel M_s is a linear Latin square and is isotopic to the addition table of $(\mathbb{Z}_k, +)$ (Corollary 8.3), hence its algebraic nature is classical [7, 5].

(2) *Integration level (new in this packaging).* The two-level orthogonal digit superposition (Sections 4–6) produces a *closed-form*, *search-free* family of *compound pandiagonal normal* magic squares of order k^2, with explicit random-access evaluation (Remark 4.9). This repackages linear Latin-square theory into an explicit constructive formula in the diabolic/pandiagonal magic-square setting initiated in [6, 14].

Acknowledgements

The author thanks the anonymous referees for their careful reading and for valuable suggestions that improved the clarity and presentation of the paper.

Conflicts of Interest

The author declares no conflict of interest.

Data Availability Statement

No new data were generated or analyzed in this study. Data sharing is not applicable to this article.

References

[1] W. S. Andrews. *Magic Squares and Cubes.* Dover Publications, New York, 1960.

[2] J. Bell and B. Stevens. Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions. *Journal of Combinatorial Designs*, 15(3):221–234, 2007. https://doi.org/10.1002/jcd.20143.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3–4):235–265, 1997. https://doi.org/10.1006/jsco.1996.0125.

[4] C. J. Colbourn and J. H. Dinitz, editors. *Handbook of Combinatorial Designs.* Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2007.

[5] J. Dénes and A. D. Keedwell. *Latin Squares and Their Applications.* Academic Press, New York, 1974.

[6] A. H. Frost. On the general properties of Nasik squares. *Quarterly Journal of Pure and Applied Mathematics*, 15:34–49, 1878.

[7] S. W. Golomb and E. C. Posner. Rook domains, Latin squares, affine planes, and error-distributing codes. *IEEE Transactions on Information Theory*, 10(3):196–208, 1964. https://doi.org/10.1109/TIT.1964.1053680.

[8] C. B. Hudson. On pandiagonal magic squares of order $6t \pm 1$. *Mathematics Magazine*, 45(2):94–96, 1972. https://doi.org/10.1080/0025570X.1972.11976202.

[9] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, Cambridge, 2nd edition, 1997.

[10] P. D. Loly and I. D. Cameron. Frierson's 1907 parameterization of compound magic squares extended to orders 3^ℓ, $\ell = 1, 2, 3, \dots$, with information entropy, 2020. https://doi.org/10.48550/arXiv.2008.11020. arXiv: 2008.11020 [math.HO].

[11] K. Ollerenshaw and D. S. Brée. *Most-perfect Pandiagonal Magic Squares: Their Construction and Enumeration.* The Institute of Mathematics and its Applications, Southend-on-Sea, 1998.

[12] K. Omori. *The World of Magic Squares (Shinban: Mahojin no Sekai).* Nippon Hyoron Sha, Tokyo, 2018. in Japanese.

[13] J. B. Rosser and R. J. Walker. On the transformation group for diabolic magic squares of order four. *Bulletin of the American Mathematical Society*, 44:414–416, 1938.

[14] J. B. Rosser and R. J. Walker. The algebraic theory of diabolic magic squares. *Duke Mathematical Journal*, 5(4):705–728, 1939. https://doi.org/10.1215/S0012-7094-39-00558-2.

[15] C.-X. Xu and Z.-W. Lu. Pandiagonal magic squares. In *Computing and Combinatorics (COCOON '95) (Xi'an, China, 1995)*, volume 959 of *Lecture Notes in Computer Science*, pages 388–391, Berlin. Springer, 1995. https://doi.org/10.1007/BFb0030856.

Osamu Shimabukuro
Department of Mathematics, Faculty of Education
Gifu Shotoku Gakuen University, Gifu 500-8288, Japan
E-mail shimabukuro@gifu.shotoku.ac.jp