Pandiagonal Sudokus

Walter Klotz

Institut für Mathematik
Technische Universität Clausthal, Germany

klotz@math.tu-clausthal.de

Torsten Sander

Fakultät für Informatik
Ostfalia Hochschule für angewandte Wissenschaften, Germany

t.sander@ostfalia.de

Submitted: Aug 1, 2011; Accepted: Jan 8, 2012; Published: Jan 16, 2012
Mathematics Subject Classification 05B15, key words: Latin square, Sudoku

Abstract

It is shown that a pandiagonal $n^2 \times n^2$-Sudoku exists if and only if $n \equiv \pm 1 \pmod 6$. Also for these n the existence of row-cyclic, pandiagonal $n^2 \times n^2$-Sudokus is conjectured and confirmed for $n = 5$ and $n = 7$.

1 Introduction

An $m \times m$-matrix $A = (a_{i,j})$ with entries from $Z_m = \{0, 1, \ldots, m-1\}$ represents a *Latin $m \times m$-square*, if every row and every column of A contains every element of Z_m exactly once (see e.g. [9]). The set of *cells* of A is

$$C(A) = Z_m \times Z_m = \{(i,j) : i \in Z_m,\ j \in Z_m\}.$$

The parallels of A to the left diagonal and to the right diagonal with parameter $h \in Z_m$ are

$$\begin{aligned} LD_h(A) &= \{(i,j) \in C(A) :\ i - j \equiv h \pmod m\}, \\ RD_h(A) &= \{(i,j) \in C(A) :\ i + j \equiv h \pmod m\}, \end{aligned} \tag{1}$$

respectively. The left diagonal of A is $LD_0(A)$, the right diagonal of A is $RD_{m-1}(A)$. The matrix A represents a *pandiagonal* Latin $m \times m$-square if every element of Z_m appears as an entry of A exactly once in every row, in every column, in every parallel to the left diagonal, and in every parallel to the right diagonal. Special pandiagonal Latin squares were considered in [1] and [4]. Hedayat [7] solved the existence problem for pandiagonal Latin squares:

Lemma 1. *A pandiagonal Latin $m \times m$-square exists, if and only if $m \equiv \pm 1$ (mod 6).*

A *region* (see [2]) of a Latin $m \times m$-square A consists of m distinct cells of A. A *regional partition* of A is a partition RP of the set $C(A)$ of all cells of A into m disjoint regions. The Latin square A is *gerecht* (German for "fair", plural is *gerechte*) with respect to RP, if every element of Z_m appears exactly once in every region of A belonging to RP (cf. [2] and [3]). Gerechte Latin squares play an important role in the design of experiments (see e.g. [5] or [8]). The complexity of constructing gerechte designs is considered in [10].

We now assume $m = n^2$. Then the n^4 cells in $C(A)$ can be partitioned into n^2 disjoint $n \times n$-*blocks*

$$B^{(s,t)} = \{(i,j) \in C(A) :\ i = sn + u,\ j = tn + v,\ 0 \leq u < n,\ 0 \leq v < n\}$$

for $0 \leq s < n$, $0 \leq t < n$. The $m \times m$-matrix A with entries from Z_m, $m = n^2$, is an $n^2 \times n^2$-*Sudoku*, if it is a Latin square which is gerecht with respect to the regional partition defined by the blocks of A. A pandiagonal Sudoku must also be gerecht with respect to the regional partition defined by the parallels to the left diagonal and by the parallels to the right diagonal. For a pandiagonal $n^2 \times n^2$-Sudoku $n \equiv \pm 1$ (mod 6) is necessary by Lemma 1. C. Boyer [6] presents a pandiagonal 25×25-Sudoku. But so far no general construction seems to be available. In Section 2 we construct pandiagonal $n^2 \times n^2$-Sudokus for every $n \equiv \pm 1$ (mod 6).

All properties of a Latin square A which we consider here are maintained if we expose the entries of A to a bijection $f : Z_m \to Z_m$. Particularly, if $A = (a_{i,j})$ is a pandiagonal Sudoku then $f(A) = (f(a_{i,j}))$ is also a pandiagonal Sudoku. The Latin $m \times m$-square is *normalized* if the entries of the first row are $0, 1, \ldots, m-1$ in their natural order. For the existence problems of the special Sudokus we investigate in Section 3 we may restrict the discussion to normalized Sudokus.

A Latin square is called *row-cyclic* if the sequence of entries of every row results from the sequence of entries of the first row by a cyclic shift. The term *column-cyclic* is defined analogously. A Latin square is *cyclic* if it is both row-cyclic and column-cyclic. We prove that no cyclic Sudoku exists, but a row-cyclic $n^2 \times n^2$-Sudoku exists for every $n \geq 2$. Our main topic in Section 3 is the existence of row-cyclic, pandiagonal $n^2 \times n^2$-Sudokus. Necessarily, $n \equiv \pm 1$ (mod 6) by Lemma 1. The case $n = 1$ is trivial. By a computer search we found out all normalized, row-cyclic, pandiagonal $n^2 \times n^2$-Sudokus for $n = 5$ and for $n = 7$. Their total number is 10 for $n = 5$, respectively 28 for $n = 7$. It turns out that all of these Sudokus can be constructed from very few (1 for $n = 5$ and 2 for $n = 7$) "basic" Sudokus by "elementary operations". It remains a challenging open problem to show the existence of row-cyclic, pandiagonal $n^2 \times n^2$-Sudokus for further $n \equiv \pm 1$ (mod 6).

2 Existence of Pandiagonal Sudokus

For the rest of this paper we assume $m = n^2$, $n \geq 1$, and $Z_m = \{0, 1, \ldots, m-1\}$. Note that, trivially, there exists a pandiagonal 1×1-Sudoku.

Lemma 2. *Let $x_0, x_1, \ldots, x_{m-1}$ be a sequence of integers in Z_m, $y \in Z_m$, $y \neq 0$, $gcd(y,n) = 1$. Suppose that the following conditions are satisfied.*

1) $x_{k+1} \equiv x_k + y \ (mod\ n)$ for every $k = 0, 1, \ldots, m-2$.

2) $k \in Z_m,\ l \in Z_m,\ k \neq l$, and $k \equiv l \ (mod\ n)$ imply $x_k \neq x_l$.

Then we have $\{x_0, x_1, \ldots, x_{m-1}\} = Z_m$.

Proof. Condition 1) implies $x_k = x_0 + ky \pmod{n}$ for $k = 0, 1, \ldots, m-1$. As y is invertible modulo n, we have for $0 \leq k < m,\ 0 \leq l < m$:

$$x_k \equiv x_l \ (\mathrm{mod}\ n) \iff k \equiv l \ (\mathrm{mod}\ n). \tag{2}$$

In particular, this means that $x_0, x_1, \ldots, x_{n-1}$ represent all residues modulo n. If we define $R_i = \{z \in Z_m : \ z = x_i \ (\mathrm{mod}\ n)\}$ then $Z_m = R_0 \cup R_1 \cup \ldots \cup R_{n-1}$ is the partition of Z_m into disjoint residue classes modulo n. For $0 \leq i < n$ we see by (2) that the integers $x_i, x_{i+n}, \ldots, x_{i+(n-1)n}$ belong to R_i. Now condition 2) implies that these integers are pairwise distinct, therefore

$$R_i = \{x_i, x_{i+n}, \ldots, x_{i+(n-1)n}\} \text{ for } 0 \leq i < n \text{ and } \bigcup_{i=0}^{n-1} R_i = \{x_0, x_1, \ldots, x_{m-1}\} = Z_m.$$

□

Each cell $(i,j) \in Z_m \times Z_m$ can also be described by 4 coordinates. Let

$$\begin{array}{lll} i = sn + u, & 0 \leq s < n, & 0 \leq u < n, \\ j = tn + v, & 0 \leq t < n, & 0 \leq v < n, \end{array} \tag{3}$$

then we call (s,t,u,v) the 4-tuple representation of (i,j). For convenience we also identify (s,t,u,v) with the corresponding cell (i,j). The cell (s,t,u,v) belongs to the block $B^{(s,t)}$, s determines the *block-row* and t the *block-column* of A.

For integers x and y, with $y > 0$, we denote by $x\%y$ the least nonnegative residue of x modulo y.

Theorem 1. *Suppose $m = n^2,\ n \geq 5,\ n \equiv \pm 1 \ (mod\ 6)$. Choose integers a and b from $\{2, \ldots, n-1\}$ such that every number $a,\ a \pm 1,\ b,\ b \pm 1$ is coprime to n. Let the cell (i,j) be represented by the 4-tuple (s,t,u,v) according to (3). Define the entry $a_{i,j}$ of the $m \times m$-Matrix A by*

$$a_{i,j} \ = \ ((au + bs + t)\%n)n + (au + v)\%n. \tag{4}$$

Then A is a normalized pandiagonal $n^2 \times n^2$-Sudoku.

Corollary 1. *A pandiagonal $n^2 \times n^2$-Sudoku exists if and only if $n \equiv \pm 1 \ (mod\ 6)$.*

The assumption $n \equiv \pm 1 \pmod{6}$ is equivalent to the condition that n has no prime divisor 2 or 3. The requirements for $a,\ a \pm 1,\ b,\ b \pm 1$ in Theorem 1 can be satisfied e.g. by choosing a and b from $\{2, 3\}$. Corollary 1 results from Theorem 1 in connection with Lemma 1, together with the fact that the case $n = 1$ is trivial.

Proof of Theorem 1. From (3) and (4) we deduce

$$a_{i,j} \equiv ai + j \pmod{n} \text{ for } 0 \le i < m,\ 0 \le j < m. \tag{5}$$

For the first row of A we have $i = s = u = 0$. Now (3) and (4) imply $a_{0,j} = j$ for $0 \le j < m$. Therefore, the first row of A has normalized form $0, 1, \ldots, m-1$. It remains to show that every row, every column, every block, and every parallel to the left/right diagonal of A contains every element of Z_m exactly once. According to these tasks we decompose the rest of the proof into four parts.

1) Rows. We partition Z_m into n disjoint intervals I_q of n successive integers:

$$I_q \ = \ \{qn,\ qn+1, \ldots,\ qn+n-1\},\ q = 0, 1, \ldots, n-1.$$

Let $x_k = a_{i,k},\ 0 \le k < m$, be the entries of row i in A. By (5) we have $x_k \equiv ai + k \pmod{n}$ for $0 \le k < m$, which shows that the sequence (x_k) satisfies condition 1) of Lemma 2 with $y = 1$.

To show that the sequence (x_k) also satisfies condition 2) of Lemma 2, let $k, l \in Z_m$, $k \ne l$, $k \equiv l \pmod{n}$. Then we have

$$k = t_1 n + v,\ l = t_2 n + v \text{ with integers } t_1, t_2, v \in \{0, 1, \ldots, n-1\},\ t_1 \ne t_2.$$

For row i the integers s and u are fixed by (3). According to (4) the integer x_k belongs to the interval I_{q_1}, $q_1 = (au + bs + t_1)\%n$, while x_l belongs to the interval I_{q_2}, $q_2 = (au + bs + t_2)\%n$. Now $t_1 \ne t_2$ implies $q_1 \ne q_2$ and $x_k \ne x_l$.

Both conditions in Lemma 2 are satisfied, therefore $\{x_0, x_1, \ldots, x_{m-1}\} = Z_m$.

2) *Columns.* Let $x_k = a_{k,j},\ 0 \le k < m$, be the entries of column j in A. By (5) we have $x_k \equiv ak + j \pmod{n}$ for $0 \le k < m$, which shows that the sequence (x_k) satisfies condition 1) of Lemma 2 with $y = a$. Here we utilize that a is coprime to n.

To show that the sequence (x_k) also satisfies condition 2) of Lemma 2, let $k, l \in Z_m$, $k \ne l$, $k \equiv l \pmod{n}$. Then we have

$$k = s_1 n + u,\ l = s_2 n + u \text{ with integers } s_1, s_2, u \in \{0, 1, \ldots, n-1\},\ s_1 \ne s_2.$$

For column j the integers t and v are fixed by (3). According to (4) the integer x_k belongs to the interval I_{q_1}, $q_1 = (au + bs_1 + t)\%n$, while x_l belongs to the interval I_{q_2}, $q_2 = (au + bs_2 + t)\%n$. Now $s_1 \ne s_2$ and b coprime to n implies $q_1 \ne q_2$ and $x_k \ne x_l$.

Both conditions in Lemma 2 are satisfied, therefore $\{x_0, x_1, \ldots, x_{m-1}\} = Z_m$.

3) *Blocks.* For the block $B^{(s,t)}$ the integers s and t in (4) are fixed. The integer u determines a row of $B^{(s,t)}$, while v determines a column of $B^{(s,t)}$. In row u of $B^{(s,t)}$ the value of $q(u) = (au+bs+t)\%n$ is fixed, while $(au+v)\%n$ assumes all values $0, 1, \dots, n-1$ for $v = 0, 1, \dots, n-1$. According to (4) this means that row u of $B^{(s,t)}$ contains exactly the numbers of the interval $I_{q(u)}$. As a is coprime to n, the term $q(u)$ assumes all values $0, 1, \dots, n-1$ for $0 \le u < n$. The set of entries of $B^{(s,t)}$ is

$$\bigcup_{u=0}^{n-1} I_{q(u)} \;=\; I_0 \cup I_1 \cup \dots \cup I_{n-1} \;=\; Z_m.$$

4) *Parallels to the left/right diagonal.* According to (1), the sequence (x_k) of entries in $LD_h(A)$, respectively $RD_h(A)$ is given by

$$x_k = a_{(h+\epsilon k)\%m,k}, \; k \in Z_m, \; \epsilon = \begin{cases} 1 & \text{for } LD_h(A) \\ -1 & \text{for } RD_h(A) \end{cases}. \tag{6}$$

From (5) we deduce

$$x_k \;\equiv\; a(h+\epsilon k) + k \pmod{n} \text{ for } 0 \le k < m,$$

which implies

$$x_{k+1} \;\equiv\; x_k + a\epsilon + 1 \pmod{n} \text{ for } 0 \le k < m-1.$$

As $a\epsilon + 1$ is coprime to n, we see that the sequence (x_k) satisfies condition 1) of Lemma 2 with $y = a\epsilon + 1$.

To confirm condition 2) of Lemma 2 we assume

$$k = t_1 n + v, \; l = t_2 n + v, \; t_1 \neq t_2, \text{ with } t_1, t_2, v \in \{0, 1, \dots, n-1\}. \tag{7}$$

By (6) we see

$$\begin{array}{lllllllll} x_k & = & a_{i,j} & \text{with} & i & = & (h+\epsilon k)\%m, & j & = & k, \\ x_l & = & a_{i',j'} & \text{with} & i' & = & (h+\epsilon l)\%m, & j' & = & l. \end{array}$$

We find integers u and w such that

$$h + \epsilon v = wn + u, \; 0 \le u < n.$$

Then we have

$$\begin{array}{lllll} i & = & (h+\epsilon v+\epsilon t_1 n)\%m & = & (u+(w+\epsilon t_1)n)\%m, \\ i' & = & (h+\epsilon v+\epsilon t_2 n)\%m & = & (u+(w+\epsilon t_2)n)\%m. \end{array}$$

This implies that i and i' have the following representations with suitable integers $s_1, \; s_2$:

$$\begin{array}{lllllll} i & = & u+s_1 n, & 0 \le s_1 < n, & s_1 & \equiv & w+\epsilon t_1 \pmod{n}, \\ i' & = & u+s_2 n, & 0 \le s_2 < n, & s_2 & \equiv & w+\epsilon t_2 \pmod{n}. \end{array}$$

We use these representations for i and i' and those for k and l in (7) to determine x_k and x_l by (4).

$$\begin{aligned} x_k &= ((au + bs_1 + t_1)\%n)n \quad + (au + v)\%n, \\ x_l &= ((au + bs_2 + t_2)\%n)n \quad + (au + v)\%n. \end{aligned}$$

Setting $q_1 = (au + bs_1 + t_1)\%n,\ q_2 = (au + bs_2 + t_2)\%n$ and inserting $s_1,\ s_2$, we achieve

$$\begin{aligned} x_k &\in I_{q_1}, \quad q_1 = (au + bw + (b\epsilon + 1)t_1)\%n, \\ x_l &\in I_{q_2}, \quad q_2 = (au + bw + (b\epsilon + 1)t_2)\%n. \end{aligned}$$

Now $q_1 = q_2$ would imply $t_1 \equiv t_2 \pmod n$, because $b\epsilon + 1$ is invertible modulo n. But this contradicts (7). So we conclude $q_1 \neq q_2$ and $x_k \neq x_l$.

Conditions 1) and 2) of Lemma 2 are satisfied, therefore $\{x_0, x_1, \ldots, x_{m-1}\} = Z_m$. □

3 Row-cyclic Pandiagonal Sudokus

In this section we will present all normalized, row-cyclic, pandiagonal $n^2 \times n^2$-Sudokus for $n = 5$ and for $n = 7$. But first we are going to disprove the existence of cyclic Sudokus for $n \geq 2$.

Throughout this section $A = (a_{i,j})$ is an $m \times m$-matrix with entries $a_{i,j} \in Z_m$, $m = n^2$. Suppose that the sequence of integers (a_k), $0 \leq k < m$, represents a permutation of the elements of Z_m. We call (a_k) *residual* (with respect to $m = n^2$) if there are integers r_s, $0 \leq r_s < n$, for $0 \leq s < n$, such that

$$a_{sn} \equiv a_{sn+1} \equiv \ldots \equiv a_{sn+n-1} \equiv r_s \pmod n \text{ for every } s = 0, 1, \ldots, n-1.$$

Observe that our assumptions imply $\{r_0, r_1, \ldots, r_{n-1}\} = \{0, 1, \ldots, n-1\}$.

Theorem 2. *Let the $m \times m$-matrix A, $m = n^2$, represent a normalized row-cyclic Latin square. Then A is an $n^2 \times n^2$-Sudoku if and only if the sequence (a_k), $0 \leq k < m$, of the entries in the first column of A is residual.*

Proof. First we assume that A is a normalized, row-cyclic $n^2 \times n^2$-Sudoku. The entries $a_0, a_1, \ldots, a_{m-1}$ of the first column of A uniquely determine every other entry of A. Fix some $s \in \{0, 1, \ldots, n-1\}$. The integers a_{sn+u}, $0 \leq u < n$, form the sequence of entries of the first column in block $B^{(s,0)}$. The set of entries in row u of $B^{(s,0)}$, $0 \leq u < n$, is

$$T_u = \{a_{sn+u}, (a_{sn+u} + 1)\%m, \ldots, (a_{sn+u} + n - 1)\%m\}.$$

As the block $B^{(s,0)}$ contains every integer in Z_m exactly once, the sets $T_0, T_1, \ldots, T_{n-1}$ constitute a partition of Z_m into disjoint subsets. Consider the element $(a_{sn} + n)\%m$ of Z_m. It does not belong to $T_0 = \{a_{sn}, (a_{sn} + 1)\%m, \ldots, (a_{sn} + n - 1)\%m\}$, but to one of the sets $T_1, T_2, \ldots, T_{n-1}$, without loss of generality

$$((a_{sn} + n)\%m) \in T_1 = \{a_{sn+1}, (a_{sn+1} + 1)\%m, \ldots, (a_{sn+1} + n - 1)\%m\}.$$

The only element $x \in T_1$ with $((x-1)\%m) \notin T_1$ is $x = a_{sn+1}$, therefore

$$((a_{sn} + n)\%m) = a_{sn+1} \text{ and } a_{sn} \equiv a_{sn+1} \pmod{n}.$$

Continuing in this way we obtain

$$a_{sn} \equiv a_{sn+1} \equiv \ldots \equiv a_{sn+n-1} \pmod{n} \text{ for every } s = 0, 1, \ldots, n-1,$$

which means that the sequence (a_k) is residual.

To prove the converse, let A be a normalized, row-cyclic Latin $m \times m$-square, $m = n^2$, with residual first column (a_k), $0 \leq k < m$. The entries b_k of column j of A, $0 \leq j < m$, are

$$b_k = (a_k + j)\%m \text{ for } 0 \leq k < m.$$

Now (a_k) residual implies (b_k) residual, so every column of A is residual.

Consider an arbitrary block $B^{(s,t)}$ of A, $0 \leq s < n$, $0 \leq t < n$. We show that $B^{(s,t)}$ contains every element of Z_m. The entries c_k in the first column of $B^{(s,t)}$ are

$$c_k = (a_{sn+k} + tn)\%m \text{ for } 0 \leq k < n.$$

The set of entries in row u of $B^{(s,t)}$, $0 \leq u < n$, is

$$M_u = \{c_u, (c_u + 1)\%m, \ldots, (c_u + n - 1)\%m\}.$$

As part of the residual column tn of A the integers $c_0, c_1, \ldots, c_{n-1}$ are distinct, but belong to the same residue class modulo n. Therefore, the sets $M_0, M_1, \ldots, M_{n-1}$ constitute a partition of Z_m into disjoint subsets. The set of entries in block $B^{(s,t)}$ is

$$M_0 \cup M_1 \cup \ldots \cup M_{n-1} = Z_m.$$

□

Corollary 2. *Let A be a normalized, row-cyclic $n^2 \times n^2$-Sudoku. Then every column of A is residual.*

Corollary 3. *Row-cyclic $n^2 \times n^2$-Sudokus exist for every $n \geq 2$, but no cyclic Sudokus.*

Proof. Assume that A is a normalized, cyclic $m \times m$-Sudoku, $m = n^2$, $n \geq 2$. By Corollary 2 the sequence of entries in every column of A has to be residual. A cyclic shift of the entries in the first column by p, $0 \leq p < m$, positions results in a residual sequence if and only if p is a multiple of n, $p = kn$, $0 \leq k < n$. As there are only n such shifts, it is not possible to generate all $m > n$ distinct columns of A by a cyclic shift from its first column.

A normalized, row-cyclic $m \times m$-Latin square A is uniquely determined by the sequence (a_k) of entries $a_0 = 0, a_2, \ldots, a_{m-1}$ in its first column. Now it is no problem to choose (a_k) residual with respect to $m = n^2$ and thus achieve that A becomes a normalized, row-cyclic Sudoku. □

We introduce numerical and positional operations on $Z^{m\times m}$, the set of all $m \times m$-matrices with entries in $Z_m = \{0, 1, \ldots, m-1\}$. Let $f : Z_m \to Z_m$ be a bijection. The *numerical operation* f on $Z^{m\times m}$ is defined by

$$f(A) = (f(a_{i,j})) \text{ for } A = (a_{i,j}) \in Z^{m\times m}.$$

Numerical operations preserve all properties described by the terms Latin square, Sudoku, row-cyclic, and pandiagonal. A simple numerical operation is defined by t_w, the additive shift by $w \in Z_m$,

$$t_w(x) = (x + w)\%m \text{ for } x \in Z_m.$$

The set of all cells associated with the matrices in $Z^{m\times m}$ is $Z_m \times Z_m$. Let $P : Z_m \times Z_m \to Z_m \times Z_m$ be a bijection. The *positional operation* P on $Z^{m\times m}$ is defined by

$$P(A) = (a_{P(i,j)}) \text{ for } A = (a_{i,j}) \in Z^{m\times m}.$$

Naturally, a numerical operation f and a positional operation P on $Z^{m\times m}$ commute, $f \circ P = P \circ f$. Here we will apply the following positional operations to $A \in Z^{m\times m}$:

RR :	reverses the order of the rows of A,
RC :	reverses the order of the columns of A,
CS_q :	induces a cyclic shift of the rows of A by q rows,
	row i becomes row $(i + q)\%m$, $0 \le q \le m$.

These operations preserve all properties described by the terms Latin square, row-cyclic, and pandiagonal. If $m = n^2$, then RR and RC map Sudoku to Sudoku. The same is true for CS_q, if $q = kn$, $0 \le k \le n$.

From now on we assume that $A = (a_{i,j}) \in Z^{m\times m}$ is a normalized and row-cyclic $m\times m$-Sudoku, $m = n^2$, $n \ge 2$. Such a Sudoku A is completely determined by the sequence $(a_i) = (a_{i,0})$ of entries in its first column,

$$a_{i,j} = (a_i + j)\%m \text{ for } i \in Z_m,\ j \in Z_m.$$

For this reason we call (a_i) the *generating sequence* of A. It is residual. We introduce special operations for A, which preserve the properties we are interested in. We define the *complement* $Comp(A)$ and the *k-partner* $P_k(A)$ for $1 \le k \le n$.

Consider the bijection $f_0 : Z_m \to Z_m$ given by $f_0(x) = (-x - 1)\%m$ for $x \in Z_m$ as a numerical operation on $Z^{m\times m}$. Then we define the complement operator by

$$Comp \;=\; f_0 \circ RC. \tag{8}$$

Proposition 1. *Let $A = (a_{i,j}) \in Z^{m\times m}$ be a normalized, row-cyclic Sudoku with generating sequence (a_i). Then $B = (b_{i,j}) = Comp(A)$ is a normalized, row-cyclic Sudoku with generating sequence (b_i),*

$$b_i = (m - a_i)\%m \text{ for } i \in Z_m.$$

If A is pandiagonal then $B = Comp(A)$ is also pandiagonal.

Proof. Clearly, $B = Comp(A) = f_0 \circ RC(A)$ is a row-cyclic Sudoku and it is pandiagonal if A is pandiagonal. As A is normalized, the sequence of entries in the first row of $RC(A)$ is $m-1, m-2, \ldots, 0$. Applying f_0, this becomes $0, 1, \ldots, m-1$, which means that B is normalized.

As A is normalized and row-cyclic the sequence of entries in the last column of A is given by $(a_i + m - 1)\%m$, $0 \leq i < m$. This is also the sequence of entries in the first column of $RC(A)$. Applying f_0, we obtain

$$b_i = (-a_i)\%m = (m - a_i)\%m \text{ for } 0 \leq i < m.$$

□

Corollary 4. *For every normalized, row-cyclic Sudoku A we have $Comp \circ Comp(A) = A$.*

Proof. $Comp \circ Comp(A)$ and A have the same generating sequence. □

Let $1 \leq k \leq n$ and $A \in Z^{m \times m}$ be a normalized, row-cyclic Sudoku with generating sequence (a_i), $w(A) = (-a_{kn-1})\%m$. The *k-partner* of A is defined by

$$P_k(A) \;=\; Comp \circ t_{w(A)} \circ CS_{kn} \circ RR(A). \tag{9}$$

Observe that the operator P_k depends on the entries of the matrix it is applied to.

Proposition 2. *Let $A = (a_{i,j}) \in Z^{m \times m}$ be a normalized, row-cyclic Sudoku with generating sequence (a_i). Then $B = P_k(A)$ has the following properties.*

a) B is a normalized and row-cyclic Sudoku.
If A is pandiagonal then B is also pandiagonal.

b) If (b_i) is the generating sequence of B, then $b_{kn-1} = a_{kn-1}$.

c) $Comp \circ P_k(A) \;=\; P_k \circ Comp(A)$.

d) $P_k \circ P_k(A) \;=\; A$.

Proof. a) Clearly, $B = P_k(A) = Comp \circ t_{w(A)} \circ CS_{kn} \circ RR(A)$ is a row-cyclic Sudoku and B is pandiagonal, if A is pandiagonal. The integer $a_{kn-1} = a_{kn-1,0}$ is the last entry in the first column belonging to the k-th block of this column. In $CS_{kn} \circ RR(A) = D$ this entry is in position $(0,0)$. The integer $w(A) = (-a_{kn-1})\%m$ is chosen such that the additive shift $t_{w(A)}$ normalizes D. But if $t_{w(A)}(D)$ is normalized, then $P_k(A) = Comp \circ t_{w(A)}(D)$ is also normalized by Proposition 1.

b) The entry in position $(kn-1, 0)$ of $CS_{kn} \circ RR(A)$ is the entry of A in position $(0,0)$, which is 0. This entry is transformed by $t_{w(A)}$ to $t_{w(A)}(0) = w(A) = (-a_{kn-1})\%m$. By Proposition 1 the application of the operator $Comp$ results in

$$b_{kn-1} = a_{kn-1}\%m = a_{kn-1}.$$

c) By Corollary 4 we know that $Comp \circ Comp$ is the identity operator. Therefore, (9) implies

$$Comp \circ P_k(A) = t_w \circ CS_{kn} \circ RR(A), \quad w = (-a_{kn-1})\%m. \tag{10}$$

We utilize that numerical and positional operations commute. The same is true for RC and CS_{kn} and also for RC and RR. Of course, $RC \circ RC$ is the identity operator.

$$\begin{aligned} P_k \circ Comp(A) =& Comp \circ t_u \circ CS_{kn} \circ RR \circ Comp(A) \\ =& f_0 \circ RC \circ t_u \circ CS_{kn} \circ RR \circ f_0 \circ RC(A) \\ =& f_0 \circ t_u \circ f_0 \circ CS_{kn} \circ RR(A) \end{aligned} \tag{11}$$

Here we have $u = (-c_{kn-1})\%m$, where c_{kn-1} is the entry of $Comp(A)$ in position $(kn-1, 0)$, which by Proposition 1 is

$$c_{kn-1} = (m - a_{kn-1})\%m \text{ , therefore } \ u = a_{kn-1}\%m = a_{kn-1}.$$

In view of (10) and (11) it remains to show

$$f_0 \circ t_u \circ f_0 = t_w.$$

For every $x \in Z_m$ we have

$$\begin{aligned} f_0 \circ t_u \circ f_0(x) &= f_0 \circ t_u((-x-1)\%m) \\ &= f_0((-x-1+u)\%m) = f_0((-x-1+a_{kn-1})\%m) \\ &= (x+1-a_{kn-1}-1)\%m = (x+w)\%m = t_w(x). \end{aligned}$$

d) According to (8) and (9) we have

$$\begin{aligned} P_k \circ P_k(A) \ &= Comp \circ t_u \circ CS_{kn} \circ RR \circ Comp \circ t_w \circ CS_{kn} \circ RR(A) \\ &= f_0 \circ RC \circ t_u \circ CS_{kn} \circ RR \circ f_0 \circ RC \circ t_w \circ CS_{kn} \circ RR(A). \end{aligned} \tag{12}$$

Here $w = (-a_{kn-1})\%m$ and $u = (-b_{kn-1})\%m$, where b_{kn-1} is the entry of $P_k(A)$ in position $(kn-1, 0)$, which by b) is $b_{kn-1} = a_{kn-1}$. It follows $u = (-a_{kn-1})\%m = w$, $t_u = t_w$. In (12) we commute operations suitably and cancel $RC \circ RC$ so that we obtain

$$P_k \circ P_k(A) \ = \ f_0 \circ t_w \circ f_0 \circ t_w \circ CS_{kn} \circ RR \circ CS_{kn} \circ RR(A). \tag{13}$$

For every $x \in Z_m$ we have $f_0 \circ t_w(x) = f_0((x+w)\%m) = (-x-w-1)\%m$ and so

$$(f_0 \circ t_w) \circ (f_0 \circ t_w)(x) = f_0 \circ t_w((-x-w-1)\%m) = (-(-x-w-1)-w-1)\%m = x.$$

Now (13) implies

$$P_k \circ P_k(A) \ = \ CS_{kn} \circ RR \circ CS_{kn} \circ RR(A).$$

If $B_1, \ldots, B_n$ is the sequence of blocks in an arbitrary block-column of A then the corresponding sequence in $CS_{kn} \circ RR(A)$ is $B'_k, B'_{k-1}, \ldots, B'_1, B'_n, B'_{n-1}, \ldots, B'_{k+1}$. Here B'_i results from B_i by reversing the order of the rows of B_i, $1 \leq i \leq n$. If we apply this operation twice to A then we end up with the original matrix A. This means $P_k \circ P_k(A) = A$. □

The notions of complement and k-partner can be transferred to *partial* Sudokus. We define a partial Sudoku by a generating sequence $a_0 = 0, a_1, \ldots, a_{qn-1}$, $1 \leq q < n$, that can be extended to a residual sequence over Z_m. The partial Sudoku generated by this sequence is the $qn \times m$-matrix $A' = (a'_{i,j})$ with entries:

$$a'_{i,j} \;=\; (a_i + j)\%m \text{ for } 0 \leq i < qn,\; 0 \leq j < m.$$

Now A' has an extension to a normalized, row-cyclic, pandiagonal $m \times m$-Sudoku, if and only if all k-partners of A', $1 \leq k \leq q$, and their complements have such an extension. This fact considerably abbreviates the search for normalized, row-cyclic, pandiagonal Sudokus.

We now present our computer results for $n = 5$ and for $n = 7$. There are exactly 10 normalized, row-cyclic, pandiagonal 25×25-Sudokus. They are given by the following generating sequences.

$$\begin{array}{rlllll}
S_1 = (0,5,10,20,15, & 8,18,13,3,23, & 17,7,2,22,12, & 6,1,16,11,21, & 14,9,19,24,4) \\
S_2 = (0,20,5,10,15, & 11,16,21,6,1, & 19,4,24,14,9, & 3,18,13,8,23, & 17,12,2,22,7) \\
S_3 = (0,20,10,5,15, & 8,3,13,18,23, & 19,24,4,14,9, & 2,12,7,22,17, & 11,1,21,16,6) \\
S_4 = (0,15,10,5,20, & 14,9,24,19,4, & 22,17,2,7,12, & 8,13,18,3,23, & 16,1,21,11,6) \\
S_5 = (0,10,5,20,15, & 9,24,19,14,4, & 23,18,8,3,13, & 6,1,11,16,21, & 17,22,2,12,7) \\
S_6 = (0,20,15,5,10, & 17,7,12,22,2, & 8,18,23,3,13, & 19,24,9,14,4, & 11,16,6,1,21) \\
S_7 = (0,5,20,15,10, & 14,9,4,19,24, & 6,21,1,11,16, & 22,7,12,17,2, & 8,13,23,3,18) \\
S_8 = (0,5,15,20,10, & 17,22,12,7,2, & 6,1,21,11,16, & 23,13,18,3,8, & 14,24,4,9,19) \\
S_9 = (0,10,15,20,5, & 11,16,1,6,21, & 3,8,23,18,13, & 17,12,7,22,2, & 9,24,4,14,19) \\
S_{10} = (0,15,20,5,10, & 16,1,6,11,21, & 2,7,17,22,12, & 19,24,14,9,4, & 8,3,23,13,18)
\end{array}$$

In the sequel we use the same notation for the sequence S_j and the Sudoku it generates. We see five complementary pairs: (S_1, S_6), (S_2, S_7), (S_3, S_8), (S_4, S_9), and (S_5, S_{10}). The k-partners of S_1 for $k = 1, 2, 3, 4$ are S_2, S_3, S_4, S_5. The 5-partner of S_1 is S_1 itself. The k-partners of S_6 for $k = 1, 2, 3, 4$ are S_7, S_8, S_9, S_{10}. The 5-partner of S_6 is S_6 itself. The sequences S_1 and S_6 have another remarkable property. We call a generating sequence $S = (a_i)$, $0 \leq i < m$, and its row-cyclic $m \times m$-Sudoku *reflexive* if

$$a_0 + a_{m-1} \equiv a_1 + a_{m-2} \equiv \ldots \equiv a_{m-1} + a_0 \pmod{m}. \tag{14}$$

If $S = (a_i)$ is reflexive then the complementary sequence $\bar{S} = ((m - a_i)\%m)$ is also reflexive. In the above list (S_1, S_6) is the only pair of complementary, reflexive sequences.

Proposition 3. *Let $S = (a_i)$, $0 \leq i < m$, be a reflexive generating sequence of the normalized, row-cyclic $m \times m$-Sudoku $A = (a_{i,j})$, $m = n^2$. Then the n-partner of A is A itself, $P_n(A) = A$.*

Proof. We determine $P_n(A)$ according to (9).

$$P_n(A) \;=\; Comp \circ t_w \circ CS_m \circ RR(A),\; w = (-a_{m-1})\%m$$

Observe that CS_m is the identity operator. The sequence of entries in the first column of $RR(A)$ is (a_{m-1-i}), $i = 0, 1, \ldots, m-1$. The additive shift t_w turns this sequence to

$$((a_{m-1-i} + w)\%m) = ((a_{m-1-i} - a_{m-1})\%m).$$

Finally, we get the generating sequence (b_i) of $P_n(A)$ by applying the *Comp* operator. According to Proposition 1 we have

$$b_i = (m - (a_{m-1-i} - a_{m-1}))\%m = (-a_{m-1-i} + a_{m-1})\%m. \tag{15}$$

We utilize the reflexivity condition (14) for (a_i):

$$a_s + a_t \equiv a_0 + a_{m-1} \equiv a_{m-1} \pmod{m} \text{ for } s, t \in Z_m \text{ with } s + t = m - 1.$$

For $s = m - 1 - i$ and $t = i$ we obtain

$$a_{m-1-i} + a_i \equiv a_{m-1},\ a_{m-1-i} \equiv a_{m-1} - a_i \pmod{m}.$$

Inserting a_{m-1-i} into (15) yields $b_i = a_i$ for every $i = 0, 1, \ldots, m-1$. The normalized, row-cyclic Sudokus $P_n(A)$ and A have the same generating sequence, therefore $P_n(A) = A$. $\square$

All 10 normalized, row-cyclic, pandiagonal 25×25-Sudokus can be reproduced from S_1 by forming the k-partners of S_1 and their complements for $k = 1, 2, 3, 4, 5$. We have a similar result for $n = 7$, $m = 49$. There are exactly 28 normalized, row-cyclic, pandiagonal 49×49-Sudokus. Among them are exactly two pairs $(T_1, \bar{T}_1)$ and $(T_2, \bar{T}_2)$ of complementary, reflexive Sudokus. All 28 normalized, row-cyclic, pandiagonal 49×49-Sudokus can be reproduced from T_1 and T_2 by forming the k-partners of T_1, T_2 and their complements for $k = 1, 2, \ldots, 7$. Here are the generating sequences of T_1 and T_2.

$$\begin{aligned} T_1 = \ & (0, 7, 28, 21, 42, 35, 14, \quad 24, 10, 38, 17, 45, 31, 3, \quad 5, 26, 47, 12, 19, 40, 33, \\ & 30, 44, 16, 2, 37, 9, 23, \quad 20, 13, 34, 41, 6, 27, 48, \quad 1, 22, 8, 36, 15, 43, 29, \\ & 39, 18, 11, 32, 25, 46, 4) \end{aligned}$$

$$\begin{aligned} T_2 = \ & (0, 14, 28, 7, 35, 42, 21, \quad 39, 25, 4, 11, 18, 46, 32, \quad 23, 37, 2, 44, 30, 9, 16, \\ & 13, 20, 48, 27, 6, 34, 41, \quad 38, 45, 24, 10, 3, 17, 31, \quad 22, 8, 36, 43, 1, 29, 15, \\ & 33, 12, 19, 47, 26, 40, 5) \end{aligned}$$

These results suggest the following

Conjecture. For every integer $n \equiv \pm 1 \pmod{6}$, $n \geq 5$, $m = n^2$, the following statements are true.

1. The set $RF(m)$ of reflexive, normalized, row-cyclic, pandiagonal $m \times m$-Sudokus is not empty.

2. The set $RF(m)$ consists of pairs of complementary Sudokus. Form a reduced set $RF_{red}(m)$ by taking only one Sudoku from each such pair. Then the set of all normalized, row-cyclic, pandiagonal $m \times m$-Sudokus is obtained by forming all k-partners, $1 \leq k \leq n$, and their complements for every Sudoku in $RF_{red}(m)$. The size of this set is $2n|RF_{red}(m)|$.

References

[1] Atkin, A. O. L., Hay, L., and Larson, R. G. Enumeration and construction of pandiagonal Latin squares of prime order. *Computers and Mathematics with Applications 9(2)* (1983), 267–292.

[2] Bailey, R. A., Cameron, P. J., and Connelly, R. Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes. *Am. Math. Monthly 115* (2008), 383–404.

[3] Behrens, W. U. Feldversuchsanordnungen mit verbessertem Ausgleich der Bodenunterschiede. *Zeitschrift für Landwirtschaftliches Versuchs- und Untersuchungswesen 2* (1956) 176–193.

[4] Bell, J., and Brett, S. Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions. *J. of Combinatorial Designs 15(3)* (2007), 221–234.

[5] Beth, T., Jungnickel, D., and Lenz, H. *Design Theory.* Cambridge University Press, 1999.

[6] Boyer, C. Smallest possible pandiagonal Sudoku. *Mathematics Today* (April 2006), page 70, available at *http://www.multimagie.com/English/SudokuPandiag.htm.*

[7] Hedayat, A. A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs. *J. Combinatorial Theory (A) 22* (1977), 331–337.

[8] Street, A. P., and Street, D. J. *Combinatorics of experimental design.* Oxford University Press, 1987.

[9] van Lint, J. H., and Wilson, R. M. *A course in combinatorics.* Cambridge University Press, 1992.

[10] Vaughan, E. R. The complexity of constructing Gerechte designs. *Electron. J. Combin. 16(1)* (2009), #R15.