involve
a journal of mathematics

Modular magic sudoku

John Lorch and Ellen Weld

msp

2012 vol. 5, no. 2

INVOLVE 5:2 (2012)
dx.doi.org/10.2140/involve.2012.5.173

Modular magic sudoku

John Lorch and Ellen Weld

(Communicated by Kenneth S. Berenhaut)

A modular magic sudoku solution is a solution to a sudoku puzzle with symbols in $\{0, 1, \ldots, 8\}$ such that rows, columns, and diagonals of each subsquare add to 0 mod 9. We count these sudoku solutions by using the action of a suitable symmetry group and we also describe maximal mutually orthogonal families.

1. Introduction

1A. ***Terminology and goals.*** Upon completing a newspaper sudoku puzzle one obtains a *sudoku solution* of order nine, namely, a nine-by-nine array in which all of the symbols $\{0, 1, \ldots, 8\}$ occupy each row, column, and subsquare. For example, both

7 2 3	1 8 5	4 6 0
4 0 5	3 2 6	1 8 7
6 1 8	4 0 7	2 3 5
1 7 0	6 3 2	5 4 8
5 4 6	8 1 0	7 2 3
8 3 2	7 5 4	0 1 6
2 6 4	0 7 8	3 5 1
3 5 7	2 6 1	8 0 4
0 8 1	5 4 3	6 7 2

and

1 8 0	7 5 6	4 2 3
2 3 4	8 0 1	5 6 7
6 7 5	3 4 2	0 1 8
8 4 6	5 1 3	2 7 0
7 0 2	4 6 8	1 3 5
3 5 1	0 2 7	6 8 4
5 1 3	2 7 0	8 4 6
4 6 8	1 3 5	7 0 2
0 2 7	6 8 4	3 5 1

(1-1)

are sudoku solutions. The righthand array in (1-1) is a *modular magic sudoku solution*: in addition to satisfying the ordinary sudoku conditions, the rows, columns, and diagonals of each subsquare add to 0 mod 9. These subsquares are called *modular magic squares*. Plain magic squares of order 3 can't be cobbled into sudoku solutions but modular magic squares can.

One of our goals is to count the modular magic sudoku solutions. In Sections 2 and 3 we discuss properties and relabelings of modular magic squares; in Section 4

MSC2010: 05B15.
Keywords: sudoku, magic square, orthogonality, Latin square.

we introduce a natural symmetry group G acting on the set X of modular magic sudoku solutions and determine its structure. These ideas, coupled with a G-invariant property possessed by certain elements of X, are used to show that there are exactly two G-orbits on X (Theorem 4.3) and that there are 32256 modular magic sudoku solutions (Theorem 4.4).

Two sudoku solutions are *orthogonal* if upon superimposition there is no repetition in the resulting ordered pairs. The set of ordered pairs formed by superimposing the righthand sudoku solution in (1-1) and the solution x_2' given in Section 5 is

10 88 01	73 52 64	46 25 37
24 33 42	87 06 15	51 60 78
65 77 56	38 41 20	02 14 83
86 44 68	50 17 32	23 71 05
72 00 27	45 63 81	18 36 54
31 55 13	04 28 76	67 82 40
53 11 35	26 74 08	80 47 62
48 66 84	12 30 57	75 03 21
07 22 70	61 85 43	34 58 16

.

One can check directly that the two solutions are orthogonal; each is called an *orthogonal mate* of the other. On the other hand, the lefthand sudoku solution in (1-1) is not orthogonal to *any* sudoku solution (or to any Latin square, for that matter). A collection of sudoku solutions is said to be *mutually orthogonal* if every pair of distinct members is orthogonal.

Another of our goals is to investigate the orthogonality of modular magic sudoku solutions. In Section 5 we show that every modular magic sudoku solution possesses an orthogonal modular magic sudoku mate and that each such pair forms a largest possible family of mutually orthogonal modular magic sudoku solutions (Theorem 5.1).

1B. ***Background: Latin squares, orthogonality, and sudoku.*** A *Latin square* of order n is an $n \times n$ array with n symbols such that every symbol appears in each row and column. Latin squares have been of mathematical interest for hundreds of years, at first in their own right (for example, Euler's 36 officers problem; see [Euler 1923; Ball and Coxeter 1987]) and then in concert with other mathematical structures when it was discovered in the early 20th century that Latin squares are intimately connected with statistical design, coding theory, finite geometry, and graph theory. (See [Colbourn and Dinitz 1996; Dénes and Keedwell 1974; Roberts 1984] for more information.) A classical theorem illustrating some of these connections, largely due to Bose [1938], is:

Theorem 1.1. *Let m be an integer with $m \geq 2$. The following are equivalent*:

(a) *There is a collection of $m-1$ mutually orthogonal Latin squares of order m.*

(b) *There is a finite projective plane of order m.*

(c) *There exists a symmetric balanced incomplete block design with the type $(m^2+m+1, m+1, 1)$.*

The theorem indicates that counting Latin squares is of fundamental importance. The exact number of Latin squares of order nine (approximately 5.52×10^{27}; see [Bammel and Rothstein 1975]) wasn't known until 1975, and the exact number for orders twelve and larger is currently unknown. Regarding families of mutually orthogonal Latin squares, it has long been known that there are at most $n-1$ mutually orthogonal Latin squares of order n and that this bound is achieved when n is a prime power. However, for nonprime power orders larger than six, the largest size of a family of mutually orthogonal Latin squares is unknown. This open problem has been proposed by Mullen [1995] as a candidate for the "next Fermat problem."

Sudoku solutions, being special types of Latin squares, inherit both the legacy and the problems associated with Latin squares. In [Felgenhauer and Jarvis 2006] and [Jarvis and Russell 2006], using computer-aided arguments, it has been shown that there are 6670903752021072936960 distinct sudoku solutions of order nine and 5472730538 orbits under the action of a natural symmetry group (consisting of rotations, relabelings, *et cetera*), respectively. Moving on to orthogonal families of sudoku solutions, it is known that there are at most $n(n-1)$ mutually orthogonal sudoku solutions of order n^2; this bound is achieved when n is a prime power. More generally it has recently been shown (for example, [Bailey et al. 2008]) that if $p_1^{k_1} \dots p_s^{k_s}$ is the prime factorization of n and $q = \min\{p_i^{k_i}\}$, then there is a family of $q(q-1)$ mutually orthogonal sudoku solutions of order n^2. As in the case of Latin squares, the maximum size of a family of mutually orthogonal sudoku solutions is unknown in general. Given the difficulty of these counting problems, it is desirable to understand tractable settings such as modular magic sudoku thoroughly so that they can be used as a testing ground for new counting methods.

1C. ***Miscellaneous remarks.*** In addition to modular magic sudoku, both *magidoku* and *quasimagic sudoku* (each described in [Forbes 2007] and certain of the latter painstakingly counted in [Jones et al. 2011]) are types of sudoku solutions characterized by additional sum conditions on the subsquares. Also, our modular magic squares are equivalent (in order three) to the pseudomagic, modular magic squares considered by Evans [1996], provided that one adds a diagonal condition to Evans' definition.

2. Properties of modular magic squares

Before investigating modular magic sudoku, we establish a few properties of modular magic squares. For example, all of the modular magic squares presented thus far have the entries $\{0, 3, 6\}$ on a diagonal; this is not coincidental. Throughout we let $U = \{1, 2, 4, 5, 7, 8\}$ and $D = \{0, 3, 6\}$ be subsets of $\{0, 1, \ldots, 8\}$, and we let the *remainder square* associated to a modular magic square consist of remainders mod 3 of the original entries. We often identify $\{0, 1, \ldots, 8\}$ with the ring $\mathbb{Z}_9$.

Lemma 2.1. *A remainder square associated to a modular magic square must be a Latin square.*

Proof. Given a modular magic square, we make the following observations about its remainder square:

(a) Each of the symbols $\{0, 1, 2\}$ must appear exactly three times in the remainder square.

(b) The rows, columns, and diagonals of the remainder square must each add to 0 mod 3 or else the rows, columns, and diagonals of the original modular magic square won't sum to 0 mod 9.

(c) No row or column can consist of the same symbol.

Item (a) must hold because there are exactly three numbers in $\mathbb{Z}_9$ possessing each of the three possible remainders mod 3. Item (b) must hold or else the rows, columns, and diagonals of the original modular magic square won't sum to 0 mod 9. Regarding item (c), rows or columns of 1s or 2s in the remainder square lead to sums of the form $7+4+1$ and $8+5+2$, respectively, in the original modular magic square; neither is equal to 0 in $\mathbb{Z}_9$. In view of items (a) and (b), a row or column of 0s in the remainder square implies a row or column of 1s, which is not allowed.

These observations imply that the remainder square is Latin: item (a) says that we have an order-three grid with three symbols each appearing three times. Further, if there is repetition of symbols in a given row or column then item (b) forces that row or column to consist of all the same symbol, thus violating item (c). □

Proposition 2.2. *In any modular magic square the elements of D must lie on a diagonal.*

Proof. We first show that the central entry of a given modular magic square must lie in D. Suppose otherwise that $\alpha \in U$ occupies the central location. Since α is not a zero divisor in $\mathbb{Z}_9$, it follows that $-(2^{-1}\alpha)$ is distinct from α. Therefore, α, $-(2^{-1}\alpha)$, and a third element of $\mathbb{Z}_9$ must form a row, column, or diagonal of the square. But the zero sum condition forces this third element to be $-(2^{-1}\alpha)$, contradicting the uniqueness of symbols in a modular magic square.

Then, given a modular magic square, the fact that an element of D lies in the center together with Lemma 2.1 indicate that the associated remainder square must be Latin with a 0 in the center. This means that all the 0s in the remainder square must occupy one of the diagonals, and so the elements of D must lie on this same diagonal in the original modular magic square. □

Finally, we observe that a modular magic square is uniquely determined by a choice of diagonal type (either "main" or "off"), elements of D to occupy this diagonal, and one element of U occupying a location away from the chosen diagonal. All of the remaining entries of the square can be filled in via the zero sum condition. This gives $2 \times 6 \times 6 = 72$ modular magic squares.

3. Modular magic relabelings

Ultimately we will use a group generated by certain grid symmetries and relabelings to count modular magic sudoku solutions. As opposed to ordinary sudoku, we cannot allow all relabelings because not every relabeling preserves modular magic squares. For example, the relabeling that swaps 0 and 1 and leaves everything else fixed is not allowable, as when

$$\begin{array}{|ccc|}\hline 4&8&6\\ 2&0&7\\ 3&1&5\\ \hline\end{array} \quad \text{becomes} \quad \begin{array}{|ccc|}\hline 4&8&6\\ 2&1&7\\ 3&0&5\\ \hline\end{array}.$$

Our purpose here is to describe the collection of *modular magic relabelings*, namely, those bijections of $\mathbb{Z}_9$ onto itself that preserve modular magic squares. We begin by making a few observations:

Lemma 3.1. *Let S denote the group of magic relabelings.*

(a) *Members of S become permutations of D when restricted to D.*

(b) *Given a permutation μ of $\{0, 3, 6\}$ and $\lambda \in U$, there is at most one $\sigma \in S$ with $\sigma|_D = \mu$ and $\sigma(\lambda) = 1$.*

(c) $|S| \leq 36$.

Proof. Part (a) must hold or else the action of such a relabeling on a modular magic square can produce a square having a member of U in its central location, contradicting Proposition 2.2. For part (b), more than one such σ would imply the existence of multiple modular magic squares possessing the data described immediately after Proposition 2.2, again a contradiction. Part (c) follows from part (b): we have $|S| \leq |S_3| \times |U| = 36$. □

Let's produce some magic relabelings. Given $k \in U$ and $l \in D$, consider the mapping $\mu_{k,l} : \mathbb{Z}_9 \to \mathbb{Z}_9$ defined by $\mu_{k,l}(n) = kn + l$. Let $H = \{\mu_{k,l} \mid k \in U, l \in D\}$,

and it is not too difficult to see that H is an order-18 subgroup of S. In addition to H there are rather less obvious magic relabelings. For example, consider the mapping $\rho : \mathbb{Z}_9 \to \mathbb{Z}_9$ defined[1] by

$$\rho(n) = \begin{cases} 2n^{-1} & \text{if } n \in U, \\ n & \text{if } n \in D. \end{cases}$$

To see that ρ preserves the magic sum property, if $m, n \in U$ and $a \in D$ with $m+n+a = 0$ (that is, $\{m, n, a\}$ make a typical row/column/diagonal triple), then

$$\begin{aligned} \rho(m) + \rho(n) + \rho(a) &= 2m^{-1} + 2n^{-1} + a \\ &= (mn)^{-1}(2m + 2n + mna) \\ &= (mn)^{-1}\big((2m + 2n + mna) + (m + n + a)\big) \\ &= (mn)^{-1}\big(3(m + n) + (mn + 1)a\big) \\ &= (mn)^{-1}(0 + 0) = 0, \end{aligned}$$

where we've used the facts that $m+n+a = 0$ in $\mathbb{Z}_9$ implies $m+n \equiv 0 \bmod 3$ and that $mn \equiv 2 \bmod 3$ for all $m, n \in U$. All told, these relabelings generate S:

Proposition 3.2. *The group S of modular magic relabelings is generated by the set $\{\mu_{k,l}, \rho \mid k \in U, l \in D\}$ and is isomorphic to $(S_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$.*

Proof. Using the fact that $\mu_{k,l} \circ \rho = \rho \circ \mu_{k^{-1},l}$, which we verify at the end of the proof, we know $H \rtimes \mathbb{Z}_2$ is a subgroup of S and so $|S| \geq 36$. But Lemma 3.1 says $|S| \leq 36$, so we conclude that $|S| = 36$ and that $S = \langle \mu_{k,l}, \rho \rangle \cong H \rtimes \mathbb{Z}_2$. Regarding H, observe that $|\mu_{1,6}| = 3$, $|\mu_{8,0}| = 2$, and $\mu_{1,6} \circ \mu_{8,0} = \mu_{8,0} \circ \mu_{1,6}^{-1}$. Therefore, these two elements generate a copy of S_3 within H. Likewise, $\mu_{4,0}$ generates a copy of $\mathbb{Z}_3$ in H that commutes with and has trivial intersection with the previously mentioned copy of S_3. Therefore, the direct product of these groups is an order-18 subgroup of H; this subgroup must be the entirety of H because $|H| = 18$. We conclude that $H \cong S_3 \times \mathbb{Z}_3$ and that $S \cong (S_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$.

Finally, we verify that $\mu_{k,l} \circ \rho = \rho \circ \mu_{k^{-1},l}$. Note that

$$\mu_{k,l} \circ \rho(n) = \begin{cases} kn + l & \text{if } n \in D, \\ 2kn^{-1} + l & \text{if } n \in U, \end{cases}$$

while

$$\rho \circ \mu_{k^{-1},l}(n) = \begin{cases} k^{-1}n + l & \text{if } n \in D, \\ 2(k^{-1}n + l)^{-1} & \text{if } n \in U. \end{cases}$$

If $n \in D$, we require $kn + l = k^{-1}n + l$ in $\mathbb{Z}_9$, or equivalently $(k - k^{-1})n = 0$ in $\mathbb{Z}_9$. The latter statement is an immediate consequence of the facts that k and k^{-1}

[1] As a product of cycles $\rho = (12)(45)(78)$.

have the same remainder mod 3 and $3|n$. If on the other hand $n \in U$, we require $(k^{-1}n+l)^{-1} = kn^{-1} + 2^{-1}l$ in $\mathbb{Z}_9$. This follows from

$$\begin{aligned}(k^{-1}n+l)(kn^{-1}+2^{-1}l) &= 1 + l\big(kn^{-1} + 2^{-1}(kn^{-1})^{-1}\big) + 2^{-1}l^2 \\ &= 1 + l(0) + 0 = 1,\end{aligned}$$

where for the latter equation $kn^{-1} + 2^{-1}(kn^{-1})^{-1} \equiv 0 \bmod 3$ and $l^2 = 0$ when $l \in D$. □

Since $|S| = 36$, all of the relabelings in part (b) of Lemma 3.1 are achieved:

Corollary 3.3. *Given $\lambda \in U$ and μ a permutation of D, there exists $\sigma \in S$ with $\sigma|_D = \mu$ and $\sigma(\lambda) = 1$.*

4. Counting modular magic sudoku solutions

We use a symmetry group G, called the *modular magic sudoku group*, to assist us in the task of counting modular magic sudoku solutions. We first describe the generators of this group and its action on the set X of modular magic sudoku solutions, then we count the number of G-orbits in X (this gives the number of "essentially different" modular magic sudoku solutions), and finally we count the total number of modular magic sudoku solutions.

4A. ***The modular magic sudoku group.*** The modular magic sudoku group G should consist of all reasonable grid transformations and relabelings that send one modular magic sudoku solution to another. We declare this group to have the generators:

- Modular magic relabelings. (Here a single relabeling is applied to each subsquare. Modular magic relabelings are discussed in Section 3 above.)
- Permutations of *large rows*. (A large row is a row of subsquares.)
- Swaps of the outer two rows within a given large row.
- Permutations of *large columns*. (A large column is a column of subsquares.)
- Swaps of the outer two columns within a large column.
- Transpose.

The first set of generators forms the group S of modular magic relabelings, whose structure we've already discussed in Section 3. The remaining generators form a group H of grid transformations (including rotations), and we have $G = H \times S$ because H, S commute and have trivial intersection.

We determine the structure of H. Observe that $H = [H_r \times H_c] \rtimes T$, where H_r denotes the subgroup of H generated by the large row and row permutations described, H_c is the analogous subgroup generated by column permutations, and

T is the two-element group generated by the transpose. The direct product arises because the groups H_r and H_c have trivial intersection and commute, while the semidirect product comes about as a result of the fact that $th_r = h_c t$ whenever t is transpose, $h_r \in H_r$, and $h_c \in H$, where h_c is obtained from h_r by simply replacing the word "row" by "column" in any generators used to produce h_r. Now H_r and H_c clearly have the same structure, so all that remains is to describe the structure of H_r, which we address in the following paragraphs.

Positions of rows within our sudoku grid can be labeled (a, b) where $a, b \in \mathbb{Z}_3$, a denotes the large row, and b denotes the row within a large row, with 1 denoting top, 0 denoting middle, and 2 denoting bottom for both large rows and rows within large rows. (This ordering of rows seems unnatural at the moment, but will suit our purpose.) The set of permutations of large rows is isomorphic to S_3, regarded as bijections of $\mathbb{Z}_3$ onto itself, with $\sigma(a, b) = \big(\sigma(a), b\big)$ for $\sigma \in S_3$. On the other hand, the set of swaps of outer rows within a given large row is isomorphic to $(\mathbb{Z}_3^*)^3 \cong \mathbb{Z}_2^3$ where if $s = (s_0, s_1, s_2) \in (\mathbb{Z}_3^*)^3$ then $s(a, b) = (a, s_a b)$.[2] (Here $s_a b$ is computed by multiplication in $\mathbb{Z}_3$.) Observe that S_3 acts on $\mathbb{Z}_2^3$ via $\sigma.s = (s_{\sigma^{-1}(0)}, s_{\sigma^{-1}(1)}, s_{\sigma^{-1}(2)})$ and that each such σ determines an automorphism $\phi_\sigma : \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$. Further, if $\sigma \in S_3$ and $s \in \mathbb{Z}_2^3$ we have the commutation relation

$$\sigma s = (\sigma.s)\sigma \tag{4-1}$$

because

$$\begin{aligned}\sigma s(a, b) &= \sigma(a, s_a b) = \big(\sigma(a), s_a b\big) = \big(\sigma(a), s_{\sigma^{-1}(\sigma(a))} b\big) \\ &= \big(\sigma(a), (\sigma.s)_{\sigma(a)} b\big) = (\sigma.s)(\sigma(a), b) = (\sigma.s)\sigma(a, b).\end{aligned}$$

An example may help: According to our labeling, the $(0, 1)$ row is the top row within the middle large row. Further, if $s = (2, 2, 1) \in (Z_3^*)^2$ and $\sigma = (021) \in S_3$, then $\sigma.s = (2, 1, 2)$. Applying these to the $(0, 1)$ row we have

$$\sigma s(0, 1) = \sigma(0, s_0 \times 1) = \sigma(0, 2 \times 1) = \sigma(0, 2) = \big(\sigma(0), 2\big) = (2, 2). \tag{4-2}$$

Therefore, the outcome of $\sigma s(0, 1)$ is the bottom row within the bottom large row. Likewise, we have

$$(\sigma.s)\sigma(0, 1) = \sigma.s(2, 1) = \big(2, (\sigma.s)_2 \times 1\big) = (2, 2 \times 1) = (2, 2), \tag{4-3}$$

with the equality of (4-2) and (4-3) as required by (4-1).

Returning to the structure of H_r, the commutation relation (4-1) implies that $H_r \cong S_3 \rtimes \mathbb{Z}_2^3$ via

$$(f, \sigma)(g, \tau) = \big(f(\sigma.g), \sigma\tau\big),$$

[2]The simple action of $s \in (\mathbb{Z}_3^*)^3$ on a row (a, b) is facilitated by the strange ordering of rows given above.

where $f, g \in (\mathbb{Z}_3^*)^3 \cong \mathbb{Z}_2^3$ and $\tau, \sigma \in S_3$. Note here that S_3 is acting on multiple copies of $\mathbb{Z}_2$ (three copies), where S_3 acts to permute the copies of $\mathbb{Z}_2$ among themselves. Semidirect products of this type are known as *wreath products*: we denote $\mathbb{Z}_2^3 \rtimes S_3$ by $\mathbb{Z}_2 \text{ wr } S_3$. Summarizing the discussion above we have:

Proposition 4.1. *The modular magic sudoku group G is isomorphic to $S \times H$, where $S \cong (S_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$ and $H \cong \left[(\mathbb{Z}_2 \text{ wr } S_3) \times (\mathbb{Z}_2 \text{ wr } S_3)\right] \rtimes \mathbb{Z}_2$. The order of this group is $|S| \times |H| = 36 \times (48 \times 48 \times 2) = 165888$.*

4B. ***Orbits of the modular magic sudoku group.*** We set about counting the G-orbits on X. Begin by declaring a modular magic sudoku solution to be in *proper form* if it has this aspect, as described by Lemma 4.2:

1 8 0 2 3 4 6 7 5	6 0 3	3 6 0
6 0 3		
3 6 0		

.

Lemma 4.2. *Every modular magic sudoku solution is in the same G-orbit as some proper form modular magic sudoku solution.*

Proof. Beginning with a modular magic sudoku solution, we apply the these group elements to produce something in proper form:

(a) Permute the large columns so that there is a 3 in the center of the upper left subsquare.

(b) Perform an outer row swap in the top large row and/or outer column swap in the left large column to place 0 in the upper right location of the upper left subsquare.

(c) Swap the middle and right large columns to place 0 in the center location of the upper middle subsquare.

(d) Make outer column swaps in the rightmost two large columns to make the $\{0, 3, 6\}$-diagonals go from lower left to upper right in the top rightmost two subsquares (rightmost two subsquares in the top large row).

(e) Swap the middle and bottom large rows so that 0 lies in the center location of the middle left subsquare (and 6 lies in the bottom left subsquare).

(f) Make outer row swaps in the bottommost two large rows to make the $\{0, 3, 6\}$-diagonals go from lower left to upper right in the leftmost bottom two subsquares (bottom two subsquares in the leftmost large column).

(g) Via Corollary 3.3 apply a modular magic relabeling to the resulting modular magic sudoku solution that fixes D and sends the upper leftmost symbol to 1. □

To count the number of proper form modular magic sudoku solutions, and thereby to determine an upper bound on the number of G-orbits, we first observe that in any proper form solution, such as

1 8 0 2 3 4 6 7 5	a_1 6 0 3	a_2 3 6 0
a_3 6 0 3		
a_4 3 6 0		

, (4-4)

each of the symbols a_1, a_2, a_3, a_4 shown in (4-4) has no more than two possible values. For example, in order for the first row to satisfy the Latin row condition, we know that a_1 and $-(a_1+6)$ cannot be 1 or 8, so $a_1 \in \{5, 7\}$. Further, one can check that values for a_1, a_2, a_3, a_4 either uniquely determine a proper form solution or lead to a contradiction of sudoku conditions. This implies that there are at most sixteen proper form solutions. A case-by-case check shows that seven of these sixteen are valid modular magic sudoku solutions and further that each of these seven is readily obtainable via G from one of the two proper form solutions:

$x_1 =$

1 8 0 2 3 4 6 7 5	7 5 6 8 0 1 3 4 2	4 2 3 5 6 7 0 1 8
7 5 6 8 0 1 3 4 2	4 2 3 5 6 7 0 1 8	1 8 0 2 3 4 6 7 5
4 2 3 5 6 7 0 1 8	1 8 0 2 3 4 6 7 5	7 5 6 8 0 1 3 4 2

and $x_2 =$

1 8 0 2 3 4 6 7 5	7 5 6 8 0 1 3 4 2	4 2 3 5 6 7 0 1 8
8 4 6 7 0 2 3 5 1	5 1 3 4 6 8 0 2 7	2 7 0 1 3 5 6 8 4
5 1 3 4 6 8 0 2 7	2 7 0 1 3 5 6 8 4	8 4 6 7 0 2 3 5 1

. (4-5)

This leads to the summary result:

Theorem 4.3. *There are exactly two G-orbits orbits in X. The modular magic sudoku solutions x_1 and x_2 can be taken as base points for these orbits.*

Proof. Our discussion up to this point indicates that there are at most two G-orbits. To finish we show that x_1 and x_2 from (4-5) must lie in different orbits. Recall that a *transversal* of a Latin square is a collection of locations that meets every row, column, and symbol exactly once. The property of possessing a transversal consisting of the diagonals of exactly three subsquares is a property that is invariant under the action of G: no modular magic sudoku group generator takes a central subsquare location to a noncentral subsquare location. We see that x_1 possesses such a transversal (the main diagonal) while x_2 does not. It follows that x_1 and x_2 must be in different G-orbits. □

4C. ***The total number of modular magic sudoku solutions.*** Let x_1 and x_2 be as in (4-5) and let G_{x_1} and G_{x_2} be the corresponding stabilizer subgroups of G (that is, $G_{x_i} = \{g \in G \mid g.x_i = x_i\}$). We introduce the notation:

- Large rows, and rows within large rows, are labeled 0, 1, and 2 from top to bottom. The same goes for columns, labeled left to right.[3]
- If σ is a permutation of $\{0, 1, 2\}$ then $\sigma_r, \sigma_c \in G$ denote the corresponding permutations of large rows and large columns, respectively, determined by σ.
- Let $s \in G$ denote the grid permutation that swaps the outer rows of every large row and the outer columns of every large column.
- Let $t \in G$ denote transpose.

We describe the structure of G_{x_1}. First observe that s is the only possible nontrivial combination of outer row/column swaps because any other nontrivial combination of these swaps when applied to x_1 yields a modular magic sudoku solution with some $\{0, 3, 6\}$ subsquare diagonal of the wrong type. This means that the possible generators of G_{x_1} have been reduced to relabelings, permutations of large rows/columns, s, and t. If $g \in G_{x_1}$ has no contribution from s or t, then the large row/column permutations must be *even*, or else $g.x_1$ is not in proper form. Likewise, if there is contribution from s or t (possibly both), then the large row/column permutations must be odd. This allows us to further narrow the possible generators for G_{x_1}, and, upon checking the possibilities, we find that all of the "allowable" large row/column permutations (in the sense of the previous two

[3]This is different from the ordering presented in Section 4A.

sentences) actually appear in elements of G_{x_1}. We therefore have

$$G_{x_1} = \langle \mu_{1,6}(012)_c,\ \mu_{1,6}(012)_r,\ \rho\mu_{5,6}(12)_r(12)_c t,\ \mu_{8,6}(12)_r(12)_c s \rangle \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2).$$

A similar analysis can be applied to G_{x_2}, which has the same "allowable" large row/column permutations, but here fewer of them actually work. Upon checking we have

$$G_{x_2} = \langle \mu_{1,6}(012)_c,\ \mu_{8,6}(12)_r(12)_c s \rangle \cong S_3,$$

a subgroup of G_{x_1}.

Theorem 4.4. *There are* 32256 *modular magic sudoku solutions.*

Proof. Let $G.x_i$ denote the G-orbit in X through x_i. From the discussion immediately above we have

$$|G.x_i| = \frac{|G|}{|G_{x_1}|} = \frac{165888}{36} = 4608 \quad \text{while} \quad |G.x_2| = \frac{|G|}{|G_{x_2}|} = \frac{165888}{6} = 27648.$$

The total number of modular magic sudoku solutions is $|G.x_1| + |G.x_2| = 32256$. □

5. Orthogonality of modular magic sudoku solutions

Here we investigate the orthogonality of modular magic sudoku solutions. We begin by observing that the solutions x_1' and x_2' given in (5-1) are modular magic and are orthogonal to the solutions x_1 and x_2 given in (4-5), respectively.

$$x_1' = \left[\begin{array}{ccc|ccc|ccc} 0&8&1 & 3&2&4 & 6&5&7 \\ 4&3&2 & 7&6&5 & 1&0&8 \\ 5&7&6 & 8&1&0 & 2&4&3 \\ \hline 6&5&7 & 0&8&1 & 3&2&4 \\ 1&0&8 & 4&3&2 & 7&6&5 \\ 2&4&3 & 5&7&6 & 8&1&0 \\ \hline 3&2&4 & 6&5&7 & 0&8&1 \\ 7&6&5 & 1&0&8 & 4&3&2 \\ 8&1&0 & 2&4&3 & 5&7&6 \end{array}\right] \quad \text{and} \quad x_2' = \left[\begin{array}{ccc|ccc|ccc} 0&8&1 & 3&2&4 & 6&5&7 \\ 4&3&2 & 7&6&5 & 1&0&8 \\ 5&7&6 & 8&1&0 & 2&4&3 \\ \hline 6&4&8 & 0&7&2 & 3&1&5 \\ 2&0&7 & 5&3&1 & 8&6&4 \\ 1&5&3 & 4&8&6 & 7&2&0 \\ \hline 3&1&5 & 6&4&8 & 0&7&2 \\ 8&6&4 & 2&0&7 & 5&3&1 \\ 7&2&0 & 1&5&3 & 4&8&6 \end{array}\right]. \quad (5\text{-}1)$$

The selection of x_1' and x_2' is not entirely random. For example, one can see that the $\{0, 3, 6\}$ subsquare diagonals for x_j and x_j' with $j \in \{1, 2\}$ must be of opposite types and that by applying a relabeling (Corollary 3.3) the upper left subsquare of

x'_j can be chosen to be

$$\begin{array}{|ccc|}\hline 0 & 8 & 1 \\ 4 & 3 & 2 \\ 5 & 7 & 6 \\ \hline \end{array}.$$

Due to the fact that orthogonality is preserved under relabelings and grid symmetries, Theorem 4.3 implies that every modular magic sudoku solution possesses an orthogonal modular magic sudoku mate.

If M is a modular magic sudoku solution let $C(M)$ denote the Latin square of order 3 with symbols in D containing the subsquare centers of M. We note that if two modular magic sudoku solutions M_1 and M_2 are orthogonal then so are $C(M_1)$ and $C(M_2)$. Since two is the maximal size of a family of mutually orthogonal Latin squares of order 3, this observation implies that the maximal size of a family of mutually orthogonal modular magic sudoku solutions is at most two. Summarizing, we have:

Theorem 5.1. *Every modular magic sudoku solution has an orthogonal modular magic sudoku mate*; *such a pair forms a largest possible family of mutually orthogonal modular magic sudoku solutions.*

References

[Bailey et al. 2008] R. A. Bailey, P. J. Cameron, and R. Connelly, "Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes", *Amer. Math. Monthly* **115**:5 (2008), 383–404. MR 2408485 Zbl 1149.05010

[Ball and Coxeter 1987] W. W. R. Ball and H. S. M. Coxeter, *Mathematical recreations and essays*, 13th ed., Dover, New York, 1987. MR 88m:00013 Zbl 0029.19701

[Bammel and Rothstein 1975] S. E. Bammel and J. Rothstein, "The number of 9×9 Latin squares", *Discrete Math.* **11**:1 (1975), 93–95. MR 51 #7882 Zbl 0304.05007

[Bose 1938] R. C. Bose, "On the application of properties of Galois fields to the problem of construction of hyper-Græco-Latin squares", *Sankhyā* **3** (1938), 323–338.

[Colbourn and Dinitz 1996] C. J. Colbourn and J. H. Dinitz (editors), *The CRC handbook of combinatorial designs*, CRC, Boca Raton, FL, 1996. MR 97a:05001 Zbl 0836.00010

[Dénes and Keedwell 1974] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, New York, 1974. MR 50 #4338 Zbl 0283.05014

[Euler 1923] L. Euler, "Recherches sur une nouvelle espèce de quarrés magiques", pp. 291–392 in *Opera omnia*, Series 1, Volume 7, Teubner, Leipzig and Berlin, 1923.

[Evans 1996] A. B. Evans, "Magic rectangles and modular magic rectangles", *J. Statist. Plann. Inference* **51**:2 (1996), 171–180. MR 97b:05035 Zbl 0851.05031

[Felgenhauer and Jarvis 2006] B. Felgenhauer and F. Jarvis, "Mathematics of sudoku I", *Math. Spectrum* **39**:1 (2006), 15–22.

[Forbes 2007] A. D. Forbes, "Quasi-magic sudoku puzzles", *M500* **215** (2007), 1–11.

[Jarvis and Russell 2006] F. Jarvis and E. Russell, "Mathematics of sudoku II", *Math. Spectrum* **39**:2 (2006), 54–58.

[Jones et al. 2011] S. K. Jones, S. Perkins, and P. A. Roach, "Properties, isomorphisms and enumeration of 2-quasi-magic sudoku grids", *Discrete Math.* **311**:13 (2011), 1098–1110. MR 2012b:05054 Zbl 1226.05064

[Mullen 1995] G. L. Mullen, "A candidate for the 'next Fermat problem'", *Math. Intelligencer* **17**:3 (1995), 18–22. MR 97a:05040 Zbl 0845.05020

[Roberts 1984] F. S. Roberts, *Applied combinatorics*, Prentice Hall, Englewood Cliffs, NJ, 1984. MR 85h:05001 Zbl 0547.05001

Received: 2011-05-02 Revised: 2011-08-24 Accepted: 2011-09-17

jlorch@bsu.edu *Department of Mathematical Sciences, Ball State University, Muncie, IN 47306, United States*

elweld@bsu.edu *Department of Mathematical Sciences, Ball State University, Muncie, IN 47306, United States*

involve

msp.berkeley.edu/involve

See inside back cover or http://msp.berkeley.edu/involve for submission instructions.

The subscription price for 2012 is US $105/year for the electronic version, and $145/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve
2012 vol. 5 no. 2