Magic Cayley-Sudoku Tables

Rosanna Mersereau  
Columbus, OH

Michael B. Ward  
Western Oregon University

1 Introduction

Inspired by the popularity of sudoku puzzles along with the well-known fact that the body of the Cayley table\(^1\) of any finite group already has \(2/3\) of the properties of a sudoku table in that each element appears exactly once in each row and in each column, Carmichael, Schloeman, and Ward \(^\text{1}\) introduced Cayley-sudoku tables. A Cayley-sudoku table of a finite group \(G\) is a Cayley table for \(G\) the body of which is partitioned into uniformly sized rectangular blocks, in such a way that each group element appears exactly once in each block. For example, Table 1 is a Cayley-sudoku table for \(\mathbb{Z}/9\) under addition mod 9 and Table 3 is a Cayley-sudoku table for \(\mathbb{Z}/3 \times \mathbb{Z}/3\) where the operation is componentwise addition mod 3 (and ordered pairs \((a, b)\) are abbreviated \(ab\)). In each case, we see that we have a Cayley table of the group partitioned into \(3 \times 3\) blocks that contain each group element exactly once.

Lorch and Weld \(^\text{3}\) defined a modular magic sudoku table as an ordinary sudoku table (with 0 in place of the usual 9) in which the row, column, diagonal, and antidiagonal sums in each \(3 \times 3\) block in the table are zero mod 9. “Magic” refers, of course, to magic Latin squares which have a rich history dating to ancient times. Table 2 is an example. Each \(3 \times 3\) block is a Latin square by the sudoku conditions and one can check that each block is a magic square when ordinary addition is replaced with addition mod 9. For example, consider the second block in the top row of blocks. The the first

\footnote{Portions of this paper are from the first author’s senior thesis at Western Oregon University.}

\footnote{That is, the operation table of the group without the borders.}
The column sum is \[7 + 8 + 3 = 0 \pmod{9}\] and the antidiagonal sum is \[6 + 0 + 3 = 0 \pmod{9}\]. Similarly, all row, column, diagonal, and antidiagonal sums in each of the blocks are \[0 \pmod{9}\], making each of them magic.

This paper aims to wed these two notions in a generalized situation. That is, we study Cayley-sudoku tables of groups (not just groups of order \(9\)) in which the blocks are magic squares with respect to “adding” the rows, columns, diagonals, and antidiagonals using the group operation. Table 3 illustrates the idea for the group \(\mathbb{Z}_3 \times \mathbb{Z}_3\). All the relevant sums in each \(3 \times 3\) block are \(0\). In fact, there is more. Each block is a pandiagonal magic square, meaning the “broken” diagonals and antidiagonals also sum to \(0\). Consider, for instance, the upper leftmost block. Beginning in the second row, first column, the broken diagonal sum is \(0 + 12 + 20 = 0\).

Although every finite group has at least one Cayley-sudoku table (see Construction 1 of [1]), not every finite group admits a magic Cayley-sudoku table. First of all, in order to partition the Cayley table into square blocks, the order of the group must be a perfect square. However, that alone is not sufficient. We will show that there is no magic Cayley-sudoku table for \(\mathbb{Z}_9\), which explains why we switched to \(\mathbb{Z}_3 \times \mathbb{Z}_3\) in order to give an example.

We do not know a characterization of groups having magic Cayley-sudoku tables. We are, however, able to give sufficient conditions which we apply to certain abelian groups, certain groups of prime power order, and which also allow us to show every finite group is isomorphic to a subgroup of a finite group admitting a magic Cayley-sudoku table.

\[
\begin{array}{c|cccc|cccc}
\hline
& 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 & 8 \\
\hline
0 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 & 8 \\
1 & 1 & 4 & 7 & 2 & 5 & 8 & 3 & 6 & 0 \\
2 & 2 & 5 & 8 & 3 & 6 & 0 & 4 & 7 & 1 \\
\hline
3 & 3 & 6 & 0 & 4 & 7 & 1 & 5 & 8 & 2 \\
4 & 4 & 7 & 1 & 5 & 8 & 2 & 6 & 0 & 3 \\
5 & 5 & 8 & 2 & 6 & 0 & 3 & 7 & 1 & 4 \\
\hline
6 & 6 & 0 & 3 & 7 & 1 & 4 & 8 & 2 & 5 \\
7 & 7 & 1 & 4 & 8 & 2 & 5 & 0 & 3 & 6 \\
8 & 8 & 2 & 5 & 0 & 3 & 6 & 1 & 4 & 7 \\
\hline
\end{array}
\]

Table 1: \(\mathbb{Z}_9\) Cayley-Sudoku Table
Table 2: Modular Magic Sudoku Table

|   | 00 | 10 | 20 | 01 | 11 | 21 | 02 | 12 | 22 |
|---|----|----|----|----|----|----|----|----|----|
| 00| 00 | 10 | 20 | 01 | 11 | 21 | 02 | 12 | 22 |
| 01| 01 | 11 | 21 | 02 | 12 | 22 | 00 | 10 | 20 |
| 02| 02 | 12 | 22 | 00 | 10 | 20 | 01 | 11 | 21 |
|10 |10 |20 |00 |11 |21 |01 |12 |22 |02 |
|11 |11 |21 |01 |12 |22 |02 |10 |20 |00 |
|12 |12 |22 |02 |10 |20 |00 |11 |21 |01 |
|20 |20 |00 |10 |21 |01 |11 |22 |02 |12 |
|21 |21 |01 |11 |22 |02 |12 |20 |00 |10 |
|22 |22 |02 |12 |20 |00 |10 |21 |01 |11 |

Table 3: Magic Cayley-Sudoku Table for $\mathbb{Z}_3 \times \mathbb{Z}_3$

2 Notation and Terminology

All groups considered herein are finite. Multiplicative notation is used for abstract groups, with 1 denoting the both the identity and the trivial subgroup $\{1\}$. For abstract group elements $a$ and $b$, $a^b$ denotes $b^{-1}ab$. When $H$ is a subgroup of $G$, we write $H \leq G$. Ordered lists of elements are indicated with square brackets, $[a, b, c, \ldots]$. Furthermore, if $L = [a_1, a_2, \ldots, a_k]$ is a list of elements in an abstract group and $b$ is a group element, then $[Lb]$ denotes the list $[a_1b, a_2b, \ldots, a_kb]$. On the other hand, when $H \leq G$, $[G : H]$ equals the index of $H$ of $G$. The exponent of $G$, $\exp(G)$, is the smallest positive integer such that $g^n = 1$ for all $g \in G$. Finally, $Z(G)$ denotes the center of $G$. 
Definitions and Background

- For \( H \leq G \) with \([G : H] = n\), if \( g_1H, g_2H, \ldots g_nH\) are all the distinct left cosets of \( H \) in \( G \), we say \( g_1, g_2, \ldots g_n\) is a **complete set of left coset representatives**\(^2\) of \( H \) in \( G \). In other words, \( g_1, g_2, \ldots g_n\) is a collection of elements, exactly one from each left coset of \( H \) in \( G \). A **complete set of right coset representatives** is defined analogously.

- In any \( k \times k \) array, a **broken diagonal** is a list of entries in positions \((\ell, \ell + j)\) where \( j \) is a fixed integer between 1 and \( k \); \( 1 \leq \ell \leq k \); and addition is mod \( k \), writing \( k \) in case of congruence to 0 mod \( k \). Similarly, a **broken antidiagonal** is a list of entries in positions \((\ell, j - \ell)\), with the same conditions on \( j \) and \( \ell \) and arithmetic mod \( k \).

  Informally, broken diagonals are parallel to the main diagonal of the square, but they wrap around when reaching a border of the square. Broken antidiagonals behave the same way with respect to the main antidiagonal. Note that \( j = k \) gives the main diagonal, while \( j = 1 \) gives the main antidiagonal. Therefore, references to broken (anti)diagonals are understood to include main (anti)diagonals as well.

- Operating elements from left to right in a row of an array of group elements is called a **row product** of the array (or **row sum** if the group is written additively).

- Operating elements from top to bottom in a column, broken diagonal, or broken antidiagonal of an array of group elements is called a **column**, **broken diagonal**, or **broken antidiagonal product**, respectively, of the array (**sum** in an additive group).

- A **Cayley-sudoku table** of a finite group \( G \) is a Cayley table for \( G \), the body of which is partitioned into uniformly sized rectangular blocks in such a way that each group element appears exactly once in each block.

- A Cayley-sudoku table is **pandiagonal magic** provided the blocks are square and every row, column, broken diagonal, and broken antidiagonal product of each of the blocks gives the group identity.

---

\(^2\)The term “left transversal” is also used. We avoid it because it has a different meaning in the theory of Latin squares.
Before proceeding, we adopt a convenient convention for labeling a Cayley table. When a list appears in a row or column of the table, it is to be interpreted as the individual elements of that list appearing (as ordered in the list) in separate rows or columns, respectively. For example, under that convention, the rows and columns of Table 1 could be labeled

\begin{align*}
\begin{array}{c|c|c}
0, 3, 6 & 1, 4, 7 & \ldots \\
0, 1, 2 & & \\
3, 4, 5 & & \\
\vdots & & \\
\end{array}
\end{align*}

Thus, the label $[0, 1, 2]$ is interpreted as the elements 0, 1, and 2 listed vertically, one per row in the indicated order, and $[0, 3, 6]$ is interpreted as the elements 0, 3, and 6 listed horizontally, one per column in the indicated order, and so forth.

For an introduction to Cayley-sudoku tables, see [1], from which we quote one construction to be used herein.

**Theorem 2.1 (Construction 1 of [1])** Let $G$ be a finite group. Assume $H$ is a subgroup of $G$ having order $k$ and index $n$ (so that $|G| = nk$). Further suppose $Hg_1, Hg_2, \ldots, Hg_n$ are the $n$ distinct right cosets of $H$ in $G$ and $T_1, T_2, \ldots, T_k$ partition $G$ into complete sets of left coset representatives of $H$ in $G$. Then, for arbitrary orderings of the elements in each right coset and in each complete set of left coset representatives, arranging the Cayley table of $G$ with columns labeled by the cosets $[Hg_1], [Hg_2], \ldots, [Hg_n]$ and the rows labeled by sets $[T_1], [T_2], \ldots, [T_k]$ (as in the table below) yields a Cayley-sudoku table of $G$ with blocks of dimension $n \times k$.

\begin{align*}
\begin{array}{c|c|c|c}
[Hg_1] & [Hg_2] & \ldots & [Hg_n] \\
T_1 & & & \\
T_2 & & & \\
\vdots & & & \\
T_k & & & \\
\end{array}
\end{align*}
3 The Principal Construction

As we shall see, the hypotheses in the following theorem are tailor made to produce the desired magic.

**Theorem 3.1 (Magic Cayley-Sudoku Construction)** Suppose

1. $G$ is a group, $|G| = k^2$, $\exp(G)$ divides $k$;
2. $N \leq Z(G)$, $|N| = k$;
3. $\prod_{\ell=1}^{k} n_\ell = 1$ where $N = [n_1, n_2, \ldots, n_k]$ (the order is unimportant since $N$ is abelian); and
4. there is a complete set of left coset representatives $T := [t_1, t_2, \ldots, t_k]$ of $N$ in $G$ such that for every $i$, $1 \leq i \leq k$, $\prod_{\ell=1}^{k} (t_\ell t_i) = t_1 t_2 t_3 \cdots t_i t_i = 1$.

Then the following is a pandiagonal magic Cayley-sudoku table.

$$
\begin{array}{|c|c|c|}
\hline
Tn_1 & [Nt_1] & [Nt_2] \\
\hline
Tn_2 & \vdots & \\
\hline
Tn_k & & [Nt_k] \\
\hline
\end{array}
$$

Table M

Henceforth, we refer to Table M as a *table of $G$ based on $N$ and $T$*.

**Proof:** It is not hard to show $Tn_1, Tn_2, \ldots, Tn_k$ partition $G$ into complete sets of left coset representatives of $N$ in $G$. Moreover, since $N$ normal subgroup of $G$, $T$ is also a complete set of right coset representatives of $N$ in $G$. By Theorem 2.1, Table M is a Cayley-sudoku table. It remains to show Table M is pandiagonal magic.

The expansion of a typical block in Table M is

$$
\begin{array}{|c|c|c|}
\hline
Tn_m & [Nt_i] & \\
\hline
\end{array} = \begin{array}{|c|c|c|}
\hline
n_1 t_i & n_2 t_i & \cdots & n_k t_i \\
\hline
\end{array},
$$
Fix \( j \) with \( 1 \leq j \leq n \).

Since \( N \leq Z(G) \), the \( j^{th} \) row product is 
\[
\prod_{\ell=1}^{k} (t_{j\ell} n_{\ell})(n_{\ell} t_{i}) = n_{m}^{k} \prod_{\ell=1}^{k} n_{\ell}(t_{j\ell} t_{i})^{k}.
\]
Furthermore, \( n_{m}^{k} = 1 = (t_{j\ell} t_{i})^{k} \) and \( \prod_{\ell=1}^{k} n_{\ell} = 1 \) by hypotheses 1 and 3 respectively. Therefore, the \( j^{th} \) row product is 1 as was to be shown.

Similarly, the \( j^{th} \) column product is 
\[
\prod_{\ell=1}^{k} (t_{\ell} n_{m})(n_{j+\ell} t_{i}) = n_{m}^{k} n_{j}^{k} \prod_{\ell=1}^{k} (t_{\ell} t_{i}) = \prod_{\ell=1}^{k} (t_{\ell} t_{i}) = 1
\]
with the last equality coming from hypothesis 4.

The broken diagonal product corresponding to \( j \) is 
\[
\prod_{\ell=1}^{k} (t_{\ell} n_{m})(n_{j-\ell} t_{i}) = n_{m}^{k} \prod_{\ell=1}^{k} n_{j-\ell}^{k} \prod_{\ell=1}^{k} (t_{\ell} t_{i}) = 1
\]
where the middle product is 1 by hypothesis 3 with the factors cyclically permuted (or because \( N \) is abelian) and, as before, the other factors are 1 by hypotheses 1 and 4. Likewise, the corresponding broken antidiagonal product is 
\[
\prod_{\ell=1}^{k} (t_{\ell} n_{m})(n_{j+\ell} t_{i}) = n_{m}^{k} \prod_{\ell=1}^{k} n_{j+\ell}^{k} \prod_{\ell=1}^{k} (t_{\ell} t_{i}) = 1
\]
(Broken diagonal and antidiagonal products were defined to be top to bottom. However, in this particular situation, calculating left to right gives the same result. For the left-to-right broken diagonal products we have 
\[
\prod_{\ell=1}^{k} (t_{\ell-\ell} n_{m})(n_{\ell} t_{i}) = n_{m}^{k} \prod_{\ell=1}^{k} n_{\ell} \prod_{\ell=1}^{k} (t_{\ell-j} t_{i}) = 1
\]
with the last equality following from hypothesis 4 with factors cyclically permuted. Left-to-right broken antidiagonal products are trivial in the same way.)

\[\square\]

4 Abelian Groups

Here we investigate the existence and nonexistence of magic Cayley-sudoku tables for certain abelian groups.
Theorem 4.1 (Abelian Groups)  Suppose

1. $G$ is an abelian group, $|G| = k^2$, exp($G$) divides $k$;
2. $N \leq G$, $|N| = k$;
3. the product of the elements of $N$ is $1$; and
4. the product of the elements of $G/N$ is $N$.

Then there is a complete set of left coset representatives, $T$, of $N$ in $G$ such that the table of $G$ based on $N$ and $T$ is a pandiagonal magic Cayley-sudoku table.

Proof. Consider any complete set of left coset representatives of $N$ in $G$, say $\{t'_1, t'_2, \ldots, t'_k\}$. By hypothesis $\prod_{\ell=1}^{k} t'_\ell N = N$, which implies there exists $n \in N$ such that $\left(\prod_{\ell=1}^{k} t'_\ell\right)n = 1$. Let $t_\ell = t'_\ell$ for $1 \leq \ell \leq k - 1$ and $t_k = t'_k n$. Clearly, $T := [t_1, t_2, \ldots, t_k]$ is a complete set of left coset representatives of $N$ in $G$ and $\prod_{\ell=1}^{k} t_\ell = 1$. We claim $T$ satisfies 4 of Theorem 3.1. For any $i$, $1 \leq i \leq k$, $\prod_{\ell=1}^{k} (t_\ell t_i) = (\prod_{\ell=1}^{k} t_\ell) t_i^k = 1$ because $G$ is abelian of exponent dividing $k$. The rest now follows from Theorem 3.1.

The following lemma shows when the hypotheses on the product of elements of $N$ and of $G/N$ in Theorem 4.1 are satisfied. We will also use it in the next section.

Lemma 4.2  Suppose $A := [g_1, g_2, \ldots, g_n]$ is an abelian finite group. Then $\prod_{\ell=1}^{n} g_\ell = 1$ if and only if $A$ either has no elements of order 2 or more than one element of order 2 (equivalently, the Sylow 2-subgroups of $A$ are trivial or non-cyclic).
Proof. The proof is elementary; see Lemma 1 of [4], for instance.

In view of Lemma 4.2, Theorem 4.1 may be applied, for example, to $G = \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ with $N = < 3 > \times \mathbb{Z}_3 \times \{0\} \times < 2 > \times < 2 >$.

We conclude this section by showing neither Theorem 4.1 nor any other method can produce a magic Cayley-sudoku table for some groups. We use those groups to illustrate the necessity of some hypotheses in Theorem 4.1.

Lemma 4.3 There is no magic Cayley-sudoku table for $\mathbb{Z}_9$ nor for $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof: Suppose to the contrary that there is a magic Cayley-sudoku table for $\mathbb{Z}_9$. The magic blocks must be $3 \times 3$. Consider the magic block intersecting the row and the column headed by 0 in the table. Let $a$ and $b$ head the remaining two columns for that block and let $x$ and $y$ label the remaining two rows. (For example, the magic block might be as below.) By the magic property, the column sums are equal. Hence, regardless of the order of the row and column labels, $x + y = x + y + 3a = x + y + 3b$, which implies $3a = 3b = 0$. Thus, $a, b \in < 3 >$. Similarly, equating the row sums yields $x, y \in < 3 >$. However, this implies all the elements of the block are in $< 3 >$ contradicting the sudoku condition that each block must contain all the elements of $\mathbb{Z}_9$.

Similarly, assume there is a magic Cayley-sudoku table for $\mathbb{Z}_2 \times \mathbb{Z}_2$. Here, the magic blocks must be $2 \times 2$. Consider the block intersecting the row and the column headed by 00 and let $a$ and $x$ head the remaining column and row in that block, respectively. Equating the 00 column and row sums in that block gives $a = x$, violating the sudoku condition.
Lemma 4.4 The hypothesis on \( \exp(G) \) cannot be omitted from Theorem 4.1. Furthermore, hypotheses 3 and 4 cannot both be omitted.

Proof: Consider the group \( G = \mathbb{Z}_3 \) with \( k = 3 \) and \( N = \langle 3 \rangle \). It is easy to show that all the hypotheses of Theorem 4.1 are satisfied except that \( \exp(G) = 9 \) does not divide 3. For example, hypothesis 4 is (because the operation is addition mod 9) \((0 + N) + (1 + N) + (2 + N) = 3 + N = N \). Therefore, by Lemma 4.3, the hypothesis on \( \exp(G) \) is necessary.

Turn now to the group \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \) with \( N = \mathbb{Z}_2 \times \{0\} \) (or any subgroup of order 2, for that matter). Neither of hypotheses 4 nor 3 are satisfied in this case, but all of the others hold. By Lemma 4.3, those hypotheses cannot both be omitted. \( \square \)

5 Other Applications

In this section, we give two more (of several possible) applications of Theorem 3.1. First, we prove every finite group is isomorphic to a subgroup of a finite group having a pandiagonal magic Cayley-sudoku table. Next, we give a class of non-abelian groups of prime power order (i.e. p-groups) having pandiagonal magic Cayley-sudoku tables.

Proposition 5.1 (Arbitrary Groups) Any finite group is isomorphic to a subgroup of a finite group having a pandiagonal magic Cayley-sudoku table.

Proof. Let \( H \) be any finite group. Define \( G := H \times H \times \mathbb{Z}_{|H|} \times \mathbb{Z}_{|H|} \) and \( N := 1 \times 1 \times \mathbb{Z}_{|H|} \times \mathbb{Z}_{|H|} \). We claim Theorem 3.1 with \( k = |H|^2 \) applies. Clearly, \( N \leq Z(G) \) and \( \exp(G) = |H| \) divides \( k \). Hypothesis 3 holds by Lemma 4.2. Take any ordering \( H = [h_1, h_2, \ldots, h_n] \) of the elements of \( H \) and define \( T \) to be the elements of \( H \times H \times 1 \times 1 \) ordered lexicographically. That is, \( (h_{i_1}, h_{j_1}, 1, 1) \) precedes \( (h_{i_2}, h_{j_2}, 1, 1) \) if and only if \( i_1 < i_2 \) or else \( i_1 = i_2 \) and \( j_1 < j_2 \). In other words, \( T := [(h_1, h_1, 1, 1), (h_1, h_2, 1, 1), \ldots, (h_1, h_n, 1, 1), (h_2, h_1, 1, 1), (h_2, h_2, 1, 1), \ldots, (h_2, h_n, 1, 1), \ldots, (h_n, h_2, 1, 1), \ldots, (h_n, h_n, 1, 1)] \). It is easy to check \( T \) is a complete set of left coset representatives of \( N \) in \( G \) since \( H \times H \times 1 \times 1 \) is a complement of \( N \) in \( G \). To check hypothesis 4, fix \( 1 \leq i, j \leq n \) and note the desired product is \( \prod_{\ell=1}^{n} (\prod_{m=1}^{n} (h_{\ell}, h_{m}, 1, 1)(h_{i}, h_{j}, 1, 1)) = \prod_{\ell=1}^{n} ((h_{\ell}h_{i})^{n}, \prod_{m=1}^{n} (h_{m}h_{j}), 1, 1) = \prod_{\ell=1}^{n} (1, \prod_{m=1}^{n} (h_{m}h_{j}), 1, 1) = (1, \prod_{m=1}^{n} (h_{m}h_{j}))^{n}, 1, 1) = (1, 1, 1, 1) \), where we used the fact that since

10
\[ n = |H|, \ h^n = 1 \] for any \( h \in H \). Thus, \( G \) has a pandiagonal magic Cayley-sudoku table and it visibly has a subgroup isomorphic to \( H \).

In the following application, the reader unfamiliar with extra-special \( p \)-groups will find all the necessary information listed in the first step of the proof.

**Proposition 5.2 (Certain \( p \)-Groups)** Suppose \( E \) is an extra-special \( p \)-group of order \( p^3 \), where \( p \) is an odd prime, and \( G = E \times \mathbb{Z}_p \). Then there is a complete set of left coset representatives, \( T \), of \( N := Z(G) \) in \( G \) such that the table of \( G \) based on \( N \) and \( T \) is a pandiagonal magic Cayley-sudoku table.

**Proof.** Assume \( p \) is an odd prime. In order to construct \( T \), some technical results about \( E \) are needed, which we number for convenience.

1. \( E \) is either \( \langle a, b : a^{p^2} = b^p = 1, ab = ba^{1+p} \rangle \), called the exponent \( p^2 \) case, or \( \langle a, b, c : a^p = b^p = c^p = 1, ac = ca, bc = cb, ab = bac \rangle \), the exponent \( p \) case. Furthermore, \( Z(E) = \langle a^p \rangle \) or \( \langle c \rangle \), in the exponent \( p^2 \) and exponent \( p \) cases, respectively. This follows from the classification of extra-special \( p \)-groups. See [2] Theorem 5.5.1, for example.

Finally, \( E/Z(E) \) is abelian since its order is \( p^2 \).

2. \( ab = baz \) for some \( z \in Z(E) \) with \( |z| = p \).

In the exponent \( p^2 \) case, \( ab = ba^{1+p} = baa^p \) and \( a^p \in Z(E) \). In the exponent \( p \) case, \( ab = bac \) and \( c \in Z(E) \). In each case, \( |z| = p \).

3. The set \( \{ b^j a^i : 0 \leq i, j \leq p-1 \} \) is a complete set of left coset representatives of \( Z(E) \) in \( E \).

First, suppose \( b^j a^i \in Z(E) \) for some \(- (p-1) \leq i, j \leq p-1 \). We aim to show \( i = j = 0 \). Using step [2] we have \( b^j a^i = (b^j a^i)^{b^{-1}} = b^j (a^{b^{-1}})^i = b^j (a z)^{i} = b^j a^i z^i \). It follows that \( 1 = z^i \), which implies \( p = |z| \) divides \( i \) and so \( i = 0 \). Therefore, \( b^j \in Z(E) \cap \langle b \rangle = 1 \), so \( p = |b| \) divides \( j \). Thus, \( j = 0 \).
Suppose $a^i b^j Z(E) = a^\ell b^m Z(E)$ where $0 \leq i, j, \ell, m \leq p - 1$, then $Z(E) = (a^i b^j)^{-1}(a^\ell b^m)Z(E) = a^{\ell-i}b^{m-j}Z(E)$, the last equality a consequence of $E/Z(E)$ being abelian. In other words, $a^{\ell-i}b^{m-j} \in Z(E)$. From the preceding paragraph, $i = \ell$ and $j = m$. Consequently, the $p^2$ elements of $\{b^j a^i : 0 \leq i, j \leq p - 1\}$ each represent a different left coset of $Z(E)$ in $E$. Since $[E : Z(E)] = p^2$, we have a complete set of left coset representatives as was to be shown.

The next three steps are easy to prove using induction. Each one uses its predecessor.

4. For every integer $i \geq 0$, $a^i b = ba^i z^i$.

5. For all integers $i, j \geq 0$, $a^i b^j = b^j a^i (z^i)^j$.

   Fix $i$ and induct on $j$.

6. For all integers $n, i, m \geq 0$,
   $$\prod_{\ell=0}^n (b^{\ell+i} a^{m}) = (\prod_{\ell=0}^n b^{\ell+i}) (a^m)^{n+1} \prod_{\ell=0}^n (z^m)^{\ell(n+i)}.$$  
   Induct on $n$.

The next step is for eventual use in proving hypothesis 4 of Theorem 3.1.

7. For all integers $i, j \geq 0$, $\prod_{k=0}^{p-1} (\prod_{\ell=0}^{p-1} (b^{\ell+k} a^i)(b^j a^i)) = 1$.

   To establish this, we begin by calculating the inner product, first uti-
lizing step 5 and, lastly, the fact that \( z \in Z(E) \) has odd order \( p \).

\[
\prod_{\ell=0}^{p-1} (b^{\ell}a^k)(b^\ell a^j) = \prod_{\ell=0}^{p-1} b^{\ell}(a^k b^\ell) a^j = \prod_{\ell=0}^{p-1} b^{\ell+i} a^k (z^k)^i a^j
\]

Further simplification follows from step 6, temporarily setting \( m := k + j \) for notational convenience. Recall that \( b \) and \( z \) each have odd order \( p \).

\[
\prod_{\ell=0}^{p-1} b^{\ell+i} a^k + j = \left( \prod_{\ell=0}^{p-1} b^{\ell+i} \right) (a^m)^p \prod_{\ell=0}^{p-1} (z^m)^{\ell+i} = b^{(p-1)p/2} a^{pm} (z^m)^{p(p-1)} a^{pm} (z^m)^{p(p-1)} z^{(p-1)p/2} = a^{pm}(z^m)^5 = a^{pm}(z^m)^2 \quad p = 3
\]

Thus, the desired double product becomes

\[
\prod_{k=0}^{p-1} \left( \prod_{\ell=0}^{p-1} (b^{\ell} a^k) (b^\ell a^j) \right) = \left\{ \begin{array}{l} \prod_{k=0}^{p-1} a^{pm}(z^m)^2 \quad p = 3 \\ \prod_{k=0}^{p-1} a^{pm} \quad p \geq 5 \end{array} \right.
\]

We split into cases. First consider the exponent \( p^2 \) case where \( z = a^p \) (see step 2).

When \( p = 3 \), \( a^{pm}(z^m)^2 = (z^m)^3 = 1 \) and we are finished. When \( p \geq 5 \), the double product is \( \prod_{k=0}^{p-1} z^m = \prod_{k=0}^{p-1} z^{k+j} = z^{(p-1)p/2 + pj} = 1 \).
Turn next to the exponent $p$ case, where $a^p = 1$. When $p \geq 5$ the double product is clearly 1. When $p = 3$, we have $\prod_{k=0}^{p-1} a^{pm}(z^m)^2 = \prod_{k=0}^{p-1}(z^{k+j})^2 = z^{(p-1)p+2pj} = 1$.

We will now show Theorem 3.1 applies with $N = Z(G) = Z(E) \times \mathbb{Z}_p$ and $k = p^2 = |N|$. First note that $\exp(G) = \exp(E)$ is either $p$ or $p^2$. The first two hypotheses of the theorem are now clear. Hypothesis 3 holds by Lemma 4.2. Let $T$ be the list $\{(b^\ell a^k, 1) : 0 \leq \ell, k \leq p - 1\}$ ordered lexicographically on $\ell$ and $k$, which is to say $(b^{\ell_1}a^{k_1}, 1)$ precedes $(b^{\ell_2}a^{k_2}, 2)$ if and only if $\ell_1 < \ell_2$ or else $\ell_1 = \ell_2$ and $k_1 < k_2$. That $T$ is a complete set of left coset representatives of $N$ in $G$ follows easily from step 3 and the fact that $N = Z(E) \times \mathbb{Z}_p$. Furthermore, $T$ satisfies Hypothesis 4 by step 7, which completes the proof. □

References

1. J. Carmichael, K. Schloeman, and M. B. Ward, Cosets and Cayley-Sudoku Tables, Math. Mag., 83 (2010) 130-139. DOI: 10.4169/002557010X482899.

2. D. Gorenstein, Finite Groups, Harper & Row, 1968.

3. J. Lorch and E. Weld, Modular Magic Sudoku, Involve 5 (2012) 173-186. DOI: 10.2140/involve.2012.5.173.

4. L. J. Paige, A Note on Finite Abelian Groups, Bull. Amer. Math. Soc. 53 (1947) 590-593. https://projecteuclid.org/euclid.bams/1183510800

14