Counting Magic Cayley-Sudoku Tables

Michael Ward
Western Oregon University

Zassenhaus Group Theory Conference
May 2015

In memory of Wolfgang Kappe

Outline

- Counting Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]

Outline

- Counting Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$

Outline

- Counting Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_3 \times \mathbb{Z}_3$

Outline

- Counting Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_3 \times \mathbb{Z}_3$
- Mutually Orthogonal Sets of Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]

Outline

- Counting Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$
- Counting Magic Cayley-Sudoku Tables for $\mathbb{Z}_3 \times \mathbb{Z}_3$
- Mutually Orthogonal Sets of Magic Sudoku Tables for $\mathbb{Z}_9$ [Lorch & Weld 2011]
- Mutually Orthogonal Sets of Magic Cayley-Sudoku Tables for $\mathbb{Z}_3 \times \mathbb{Z}_3$

Definitions

A **Sudoku Table** for $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ is a 9×9 array partitioned into 3×3 blocks in which the elements of $\mathbb{Z}_9$ appear exactly once in each row and column (Latin square) and in each block (sudoku puzzle).

Such a table is **Magic** if the row, column, and diagonal sums in each 3×3 block are zero mod 9.

Magic Sudoku Table for $\mathbb{Z}_9$

Example

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

Sales Pitch & Question

9×9 Latin Square Count

"The exact number of Latin squares of order 9 (approximately 5.52×10^{27}) wasn't known until 1975, and the exact number for orders twelve and larger is currently unknown." [Lorch & Weld]

Sales Pitch & Question

9×9 Latin Square Count

"The exact number of Latin squares of order 9 (approximately 5.52×10^{27}) wasn't known until 1975, and the exact number for orders twelve and larger is currently unknown." [Lorch & Weld]

Sudoku Table Count

The exact number of Sudoku Tables for $\mathbb{Z}_9$ is approximately 6.67×10^{21}, evidently known only via computer.

Sales Pitch & Question

9×9 Latin Square Count

"The exact number of Latin squares of order 9 (approximately 5.52×10^{27}) wasn't known until 1975, and the exact number for orders twelve and larger is currently unknown." [Lorch & Weld]

Sudoku Table Count

The exact number of Sudoku Tables for $\mathbb{Z}_9$ is approximately 6.67×10^{21}, evidently known only via computer.

Question

How many Magic Sudoku Tables are there for $\mathbb{Z}_9$?

Lorch & Weld Counting

- Let $\mathscr{M}$ be the set of Magic Sudoku Tables for $\mathbb{Z}_9$.

Lorch & Weld Counting

- Let $\mathscr{M}$ be the set of Magic Sudoku Tables for $\mathbb{Z}_9$.
- Find a group acting on $\mathscr{M}$ with few orbits. Add up the orbit lengths.

Lorch & Weld Counting

- Let $\mathscr{M}$ be the set of Magic Sudoku Tables for $\mathbb{Z}_9$.
- Find a group acting on $\mathscr{M}$ with few orbits. Add up the orbit lengths.
- L & W construct a group of order $2^{11}3^4$ with 2 orbits.

Lorch & Weld Counting

- Let $\mathscr{M}$ be the set of Magic Sudoku Tables for $\mathbb{Z}_9$.
- Find a group acting on $\mathscr{M}$ with few orbits. Add up the orbit lengths.
- L & W construct a group of order $2^{11}3^4$ with 2 orbits.
- Stabilizers have orders $2^2 3^2$ and $2 \cdot 3$.

Lorch & Weld Counting

- Let $\mathscr{M}$ be the set of Magic Sudoku Tables for $\mathbb{Z}_9$.
- Find a group acting on $\mathscr{M}$ with few orbits. Add up the orbit lengths.
- L & W construct a group of order $2^{11}3^4$ with 2 orbits.
- Stabilizers have orders $2^2 3^2$ and $2 \cdot 3$.
- $|\mathscr{M}| = \dfrac{2^{11}3^4}{2^2 3^2} + \dfrac{2^{11}3^4}{2 \cdot 3} = 32,256.$

Definitions

A **Cayley-Sudoku Table** for $\mathbb{Z}_9$ [C-S Table] is a Cayley table which is also a (bordered) Sudoku table.

	0	3	6	1	4	7	2	5	8
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
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
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

Such a table is **Magic** if the row, column, and diagonal sums in each 3×3 block is zero mod 9.

Counting

- How many Magic Cayley-Sudoku Tables [MC-S Tables] for $\mathbb{Z}_9$?

Counting

- How many Magic Cayley-Sudoku Tables [MC-S Tables] for $\mathbb{Z}_9$?
- **Lemma** None!

Counting

- How many Magic Cayley-Sudoku Tables [MC-S Tables] for $\mathbb{Z}_9$?
- **Lemma** None!
- Switch groups to $\mathbb{Z}_3 \times \mathbb{Z}_3 := \mathbb{Z}_3^2$.

Constructing Magic Cayley-Sudoku Tables for $\mathbb{Z}_3 \times \mathbb{Z}_3$

Choose any two complementary subgroups of order 3, $U =< u >$ and $V =< v >$, $U \times V = \mathbb{Z}_3 \times \mathbb{Z}_3$ (multiplicative notation).
“Large columns" indexed by cosets of U. Columns within each large column labeled with elements of its coset.
Large rows and rows similarly labeled using cosets of V.

		U			vU			v^2U		
		1	u	u^2	v	vu	vu^2	v^2	v^2u	v^2u^2
V	1	1	u	u^2	v	vu	vu^2	v^2	v^2u	v^2u^2
	v	v	vu	vu^2	v^2	v^2u	v^2u^2	1	u	u^2
	v^2	v^2	v^2u	v^2u^2	1	u	u^2	v	vu	vu^2
Vu	u	u	u^2	1	vu	vu^2	v	v^2u	v^2u^2	v^2
	vu	vu	vu^2	v	v^2u	v^2u^2	v^2	u	u^2	1
	v^2u	v^2u	v^2u^2	v^2	u	u^2	1	vu	vu^2	v
Vu^2	u^2	u^2	1	u	vu^2	v	vu	v^2u^2	v^2	v^2u
	vu^2	vu^2	v	vu	v^2u^2	v^2	v^2u	u^2	1	u
	v^2u^2	v^2u^2	v^2	v^2u	u^2	1	u	vu^2	v	vu

Characterization

Any permutation of the large columns [rows] yields another MC-S Table.
Within any large column [row], any permutation of the columns [rows] yields another MC-S Table.

Characterization

Any permutation of the large columns [rows] yields another MC-S Table.
Within any large column [row], any permutation of the columns [rows] yields another MC-S Table.

Theorem *Every MC-S Table for* $\mathbb{Z}_3^2$ *is obtained in this way for some choice of* U *and* V.

Characterization

Any permutation of the large columns [rows] yields another MC-S Table.
Within any large column [row], any permutation of the columns [rows] yields another MC-S Table.

Theorem *Every MC-S Table for* $\mathbb{Z}_3^2$ *is obtained in this way for some choice of* U *and* V.

Any of the MC-S Tables so constructed from a given U and V we call a (U, V)-table.

Plain Counting

4	Choices for $U =< u >$
3	Choices for $V =< v >$
3!	Arrangements of large columns (indexed by U, vU, v^2U)
$(3!)^3$	Arrangements of columns within large columns
3!	Arrangements of large rows (indexed by V, Vu, Vu^2)
$(3!)^3$	Arrangements of rows within large rows
$12 \cdot (3!)^8$	Magic Cayley-Sudoku Tables for $\mathbb{Z}_3^2$

$12 \cdot (3!)^8 = 20,155,392$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows
- $R \cong S_3 \wr S_3$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows
- $R \cong S_3 \wr S_3$
- L := the group of relabelings, i.e. bijections from $\mathbb{Z}_3^2$ to itself that preserve MC-S Tables

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows
- $R \cong S_3 \wr S_3$
- L := the group of relabelings, i.e. bijections from $\mathbb{Z}_3^2$ to itself that preserve MC-S Tables
- $L \cong \mathrm{Aut}(\mathbb{Z}_3^2) \cong \mathrm{GL}(2,3)$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows
- $R \cong S_3 \wr S_3$
- L := the group of relabelings, i.e. bijections from $\mathbb{Z}_3^2$ to itself that preserve MC-S Tables
- $L \cong \mathrm{Aut}(\mathbb{Z}_3^2) \cong \mathrm{GL}(2,3)$
- Set $G = L \times C \times R \cong \mathrm{GL}(2,3) \times (S_3 \wr S_3) \times (S_3 \wr S_3)$

Fancy Counting à la Lorch & Weld

- $\mathscr{M}$:= the set of MC-S Tables for for $\mathbb{Z}_3^2$
- C := group of permutations of large columns and columns within large columns
- $C \cong S_3 \wr S_3$
- R := group of permutations of large rows and rows within large rows
- $R \cong S_3 \wr S_3$
- L := the group of relabelings, i.e. bijections from $\mathbb{Z}_3^2$ to itself that preserve MC-S Tables
- $L \cong \mathrm{Aut}(\mathbb{Z}_3^2) \cong \mathrm{GL}(2,3)$
- Set $G = L \times C \times R \cong \mathrm{GL}(2,3) \times (S_3 \wr S_3) \times (S_3 \wr S_3)$
- $|G| = 48 \cdot (3!)^8$

Fancy Counting Continued

Lemma G acts transitively on $\mathscr{M}$ and $|G_M| = 4$ for any $M \in \mathscr{M}$.

Fancy Counting Continued

Lemma G acts transitively on $\mathscr{M}$ and $|G_M| = 4$ for any $M \in \mathscr{M}$.

Proof. Let $M_i \in \mathscr{M}$, M_i a (U_i, V_i)-table for $i = 12$.
For some $\sigma \in \mathrm{GL}(2,3)$, $U_1^\sigma = U_2$ and $V_1^\sigma = V_2$
M_1^σ is a (U_2, V_2)-table.
Permute rows and columns with an element of $C \times R$ to match M_2.

Fancy Counting Continued

Lemma G acts transitively on $\mathscr{M}$ and $|G_M| = 4$ for any $M \in \mathscr{M}$.

Proof. Let $M_i \in \mathscr{M}$, M_i a (U_i, V_i)-table for $i = 12$.
For some $\sigma \in \mathrm{GL}(2,3)$, $U_1^\sigma = U_2$ and $V_1^\sigma = V_2$
M_1^σ is a (U_2, V_2)-table.
Permute rows and columns with an element of $C \times R$ to match M_2.

Fix $M \in \mathscr{M}$, M_i a (U, V)-table, $U =< u >$, $V =< v >$.
$\sigma \in \mathrm{GL}(2,3)$, $\rho \in C \times R$,
$\sigma\rho \in G_M \Rightarrow U^\sigma = U, v^\sigma = V \Rightarrow u^\sigma = u^{\pm 1}, v^\sigma = v^{\pm 1}$
For each such σ there is a unique ρ such that $\sigma\rho$ fixes M.

Fancy Counting Continued

Lemma G acts transitively on $\mathscr{M}$ and $|G_M| = 4$ for any $M \in \mathscr{M}$.

Proof. Let $M_i \in \mathscr{M}$, M_i a (U_i, V_i)-table for $i = 12$.
For some $\sigma \in \mathrm{GL}(2,3)$, $U_1^\sigma = U_2$ and $V_1^\sigma = V_2$
M_1^σ is a (U_2, V_2)-table.
Permute rows and columns with an element of $C \times R$ to match M_2.

Fix $M \in \mathscr{M}$, M_i a (U, V)-table, $U =< u >$, $V =< v >$.
$\sigma \in \mathrm{GL}(2,3)$, $\rho \in C \times R$,
$\sigma\rho \in G_M \Rightarrow U^\sigma = U, v^\sigma = V \Rightarrow u^\sigma = u^{\pm 1}, v^\sigma = v^{\pm 1}$
For each such σ there is a unique ρ such that $\sigma\rho$ fixes M.

Corollary $|\mathscr{M}| = \dfrac{|G|}{|G_M|} = \dfrac{48 \cdot (3!)^8}{4} = 12 \cdot (3!)^8 = 20,155,393.$

Orthogonality

Definition

*Two Latin squares are **orthogonal** provided each ordered pair of symbols occurs exactly once when the squares are superimposed.*
*A family of Latin squares is **mutually orthogonal** provided each pair of distinct elements are orthogonal.*

Orthogonality

Definition

Two Latin squares are ***orthogonal*** *provided each ordered pair of symbols occurs exactly once when the squares are superimposed.*
A family of Latin squares is ***mutually orthogonal*** *provided each pair of distinct elements are orthogonal.*

Example

These Cayley tables of $\mathbb{Z}_3$ *are orthogonal.*

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

	0	1	2
0	0	1	2
2	2	0	1
1	1	2	0

00	11	22
12	20	01
21	02	10

Sales Pitch & Questions

The next Fermat problem?

"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 [i.e. $n \times n$], and that this bound is achieved when n is a prime power. However, for non-prime power orders larger than six, the largest size of a family of mutually orthogonal latin squares is unknown. This problem has been proposed by Mullen as a candidate for the 'next Fermat problem.'" [Lorch & Weld]

Sales Pitch & Questions

The next Fermat problem?

"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 [i.e. $n \times n$], and that this bound is achieved when n is a prime power. However, for non-prime power orders larger than six, the largest size of a family of mutually orthogonal latin squares is unknown. This problem has been proposed by Mullen as a candidate for the 'next Fermat problem.'" [Lorch & Weld]

So the largest size of a mutually orthogonal family of 9×9 Latin squares is 8.

Sales Pitch & Questions

The next Fermat problem?

"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 [i.e. $n \times n$], and that this bound is achieved when n is a prime power. However, for non-prime power orders larger than six, the largest size of a family of mutually orthogonal latin squares is unknown. This problem has been proposed by Mullen as a candidate for the 'next Fermat problem.'" [Lorch & Weld]

So the largest size of a mutually orthogonal family of 9×9 Latin squares is 8.

Questions

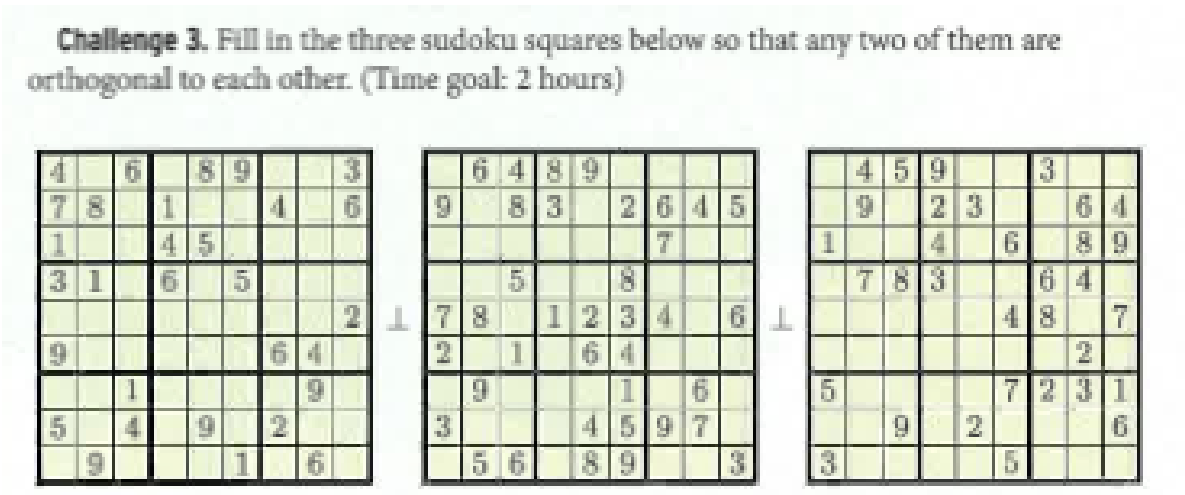
What is the largest size of a mutually orthogonal family of Sudoku Tables & Magic Sudoku Tables for $\mathbf{Z}_9$? Magic Cayley-Sudoku Tables for $\mathbf{Z}_3^2$?

Mutually Orthogonal Sets of Sudoku Tables for $\mathbb{Z}_9$

Theorem (Pedersen & Vis, 2009)

There exists a family of 6 mutually orthogonal Sudoku Tables for $\mathbb{Z}_9$ and this is the largest possible such family.

———————O———————



Orthogonal Sudoku Puzzle (MAA FOCUS)

Mutually Orthogonal Sets of Magic Sudoku Tables for $\mathbb{Z}_9$

Theorem (Lorch & Weld)

There exists a family of 2 mutually orthogonal Magic Sudoku Tables for $\mathbb{Z}_9$ and this is the largest possible such family.

Mutually Orthogonal Sets of Magic-Cayley Sudoku Tables for $\mathbb{Z}_3^2$

Theorem

There exists a family of 6 mutually orthogonal Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$ and this is the largest possible such family, assuming any such family can be normalized to have the same column labels.

Mutually Orthogonal Sets of Magic-Cayley Sudoku Tables for $\mathbb{Z}_3^2$

Theorem

There exists a family of 6 mutually orthogonal Magic Cayley-Sudoku Tables for $\mathbb{Z}_9$ and this is the largest possible such family, assuming any such family can be normalized to have the same column labels.

Idea of the Proof (adapted from Pedersen & Vis)

Think of $\mathbb{Z}_3^2$ as the additive group of GF(9). Take $U = \mathrm{GF}(3)$. For each $x \in \mathrm{GF}(9) \setminus U$, Ux is a complement to U. A family of (U, Ux)-tables, one for each $x \in \mathrm{GF}(9) \setminus U$, suitably arranged, is mutually orthogonal.

References

1. J. Lorch and E. Weld, Modular Magic Sudoku, `http://www.cs.bsu.edu/homepages/jdlorch/mmsarticle.pdf`
2. G. L. Mullen, A candidate for the “next Fermat problem," *Math. Intelligencer* **17** 18-22.
3. R. M. Pedersen and T. L. Vis, Sets of Mutually Orthogonal Sudoku Latin Squares, *College Math. J.* **40** (2009) 174-180.