Math/CS 103 Professor: Padraic Bartlett

# Minilecture 7: Magic Squares

*Week 5* *UCSB 2014*

Today's application is to magic! Not the friendship kind, though; instead, we're going to talk about **magic squares**, an incredibly old piece of mathematics that we can study using Latin squares.

## 1 Magic Squares

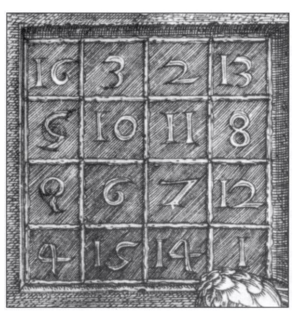
**Definition.** A **magic square** is a $n \times n$ grid filled with the integers $\{0, 1, \dots n^2 - 1\}$, such that

- each number is used exactly once in our entire grid, and
- the sum of all of the entries along any row, column, the main diagonal[1] or the main antidiagonal all come out to the same constant value.

Here's an example for order 3:

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

Magic squares have been studied for a fairly ridiculously long time. Mathematicians and philosophers were aware of them since about 650 BC; since their discovery, people have used them both as the basis for magic tricks (when your population is largely numerically illiterate, magic squares were a neat way to perform seemingly impossible feats) and religious/spiritual/cultural icons.




(A zoomed-in portion of an engraving by Albrecht Dürer, titled *Melencolia I*. Note how he hid the year of his engraving, 1514, in the last row.)

[1]The main diagonal of a $n \times n$ grid is simply the set of cells connecting the top-left to the bottom-right cells: i.e. $(1, 1), (2, 2), \dots (n, n)$. Similarly, the main antidiagonal is just the set of cells connecting the bottom-left to the top-right: i.e. $(n, 1), (n - 1, 2), \dots (1, n)$.

As mathematicians, our first impulse upon seeing a new definition is to ask "When do these things exist?" By doing some scratchwork, we can show that these don't exist for order 2: this is because every grid we can make will look like either $\begin{array}{|c|c|}\hline 0 & 2 \\ \hline 3 & 1 \\ \hline\end{array}$ or $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 3 & 1 \\ \hline\end{array}$ or $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 2 & 3 \\ \hline\end{array}$, by rotating it so that 0 is in the upper-left corner and flipping it so that the entry in the upper-right is greater than the one in the lower-left. None of these are magic: therefore, there is no magic square of order 2.

There is one of order 1 (Behold: $\boxed{0}$ !), and we've already shown that ones exist of order 3 and 4. However, we haven't really introduced a method for looking for these yet; we've just sort of given some examples, most of which we made by just picking numbers.

Surprisingly, we can create these objects using Latin squares! We describe the method here:

## 2 Diagonal Latin Squares

**Definition.** A **diagonal Latin square** is a Latin square such that its main diagonal contains no repeated symbols, and similarly its main antidiagonal also does not contain any repeated symbols.

We can easily make one of order 1 (Behold: $\boxed{1}$ !), and can easily see that we cannot do this for order 2: if we take a $2 \times 2$ Latin square with the symbols $1, 2$ on the diagonal, i.e. $\begin{array}{|c|c|}\hline 1 & \phantom{0} \\ \hline \phantom{0} & 2 \\ \hline\end{array}$, there's clearly no way to complete this to a Latin square.

Similarly, if we take a $3 \times 3$ partial Latin square with $1, 2, 3$ on the diagonal (without any loss of generality, in the order $(1, 2, 3)$), we can see that there is only one way to fill it in:

$$\begin{array}{|c|c|c|}\hline 1 & & \\ \hline & 2 & \\ \hline & & 3 \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 1 & & \\ \hline & 2 & \color{red}{1} \\ \hline & \color{red}{1} & 3 \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 1 & \color{red}{3} & \color{red}{2} \\ \hline \color{red}{3} & 2 & \color{red}{1} \\ \hline \color{red}{2} & \color{red}{1} & 3 \\ \hline\end{array}.$$

This square does not contain the symbols $1, 2, 3$ on its antidiagonal; therefore, there is no diagonal Latin square of order 3.

Conversely, using the same method of "just try it" gives us a way to explicitly find a diagonal Latin square of order 4: if we attempt to put the symbols $1 \ldots 4$ on the diagonal, we can try to put 3 in the cells $(1, 2), (2, 1)$,

$$\begin{array}{|c|c|c|c|}\hline 1 & & & \\ \hline & 2 & & \\ \hline & & 3 & \\ \hline & & & 4 \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1 & \color{red}{3} & & \\ \hline \color{red}{3} & 2 & & \\ \hline & & 3 & \\ \hline & & & 4 \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1 & \color{red}{3} & \color{red}{4} & \color{red}{2} \\ \hline \color{red}{3} & 2 & \color{red}{?} & \color{red}{1} \\ \hline & & 3 & \\ \hline & & & 4 \\ \hline\end{array}$$

in which case we fail. Alternately, we can try to put 3 in $(1, 2)$ and 4 in $(2, 1)$, in which case we have

$$\begin{array}{|c|c|c|c|}\hline 1 & & & \\ \hline & 2 & & \\ \hline & & 3 & \\ \hline & & & 4 \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1 & 3 & & \\ \hline 4 & 2 & & \\ \hline & & 3 & \\ \hline & & & 4 \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 2 \\ \hline 4 & 2 & 1 & 3 \\ \hline 2 & 4 & 3 & 1 \\ \hline 3 & 1 & 2 & 4 \\ \hline \end{array},$$

which works! So we've found one for order 4.

However, this ad-hoc approach is unsatisfying: when will it work? How can we do this efficiently; i.e. without having to run into dead ends, or with a guarantee that our process will work?

There are a number of constructions that mathematicians have came up with over time. One of my favorites, b/c of its simplicity, is the following:

**Construction.** Take any value of $n$, and any two numbers $a, b \in \{0, \dots n-1\}$. Consider the following square populated with the elements $\{0, 1 \dots n-1\}$:

$$L = \begin{array}{|c|c|c|c|c|c|}\hline 0 & a & 2a & 3a & \dots & (n-1)a \\ \hline b & b+a & b+2a & b+3a & \dots & b+(n-1)a \\ \hline 2b & 2b+a & 2(b+a) & 2b+3a & \dots & 2b+(n-1)a \\ \hline 3b & 3b+a & 3b+2a & 3(b+a) & \dots & 3b+(n-1)a \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline (n-1)b & (n-1)b+a & (n-1)b+2a & (n-1)b+3a & \dots & (n-1)(b+a) \\ \hline \end{array} \mod n.$$

In other words, $L$'s $(i, j)$-th cell contains the symbol given by taking the quantity $ai + bj \mod n$.

This construction, made by filling in the cells $(i, j)$ of our Latin square using some linear map $ai + bj$, should feel familiar to you: it is the same kind of map we used when we turned finite fields into Latin squares, and it is also the same kind of map we used when we turned affine planes into Latin squares, kinda (i.e. the same idea of parallel lines becoming Latin squares showed up in both of these things.)

Given this construction, a question we'd like to ask is the following: for what values of $n$ is this a diagonal Latin square?

This is your first HW problem!

Your second HW problem is to prove the following:

**Proposition.** Given a Latin square $L$ produced by the above process, the transpose[2] $L^T$ is also a diagonal Latin square, and is furthermore orthogonal to $L$.

Here's your third problem:

**Proposition.** Take any pair of orthogonal diagonal $n \times n$ Latin squares $L_1, L_2$ on the symbols $\{0, \dots n-1\}$. Create the square $M$ as follows: if the cell $(i, j)$ contains the symbol $x$ in $L_1$, $y$ in $L_2$, write down the number $nx + y$ in the cell $(i, j)$ of $M$. This square $M$ is a magic square.

[2] The **transpose** of an $n \times n$ array is what you get when you "flip" your array over its main diagonal.