Lecture 5: Latin Squares and Magic

Today's application is to magic! Not the friendship kind, though[1]; 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

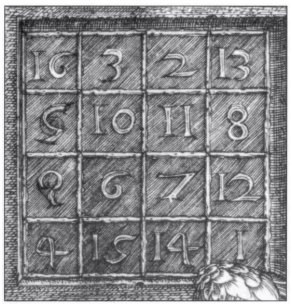
Definition. A **magic square** is a $n \times n$ grid filled with the integers $\{0, 1, \dots n^2 - 1\}$, such that

- 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[2] 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] Fluttershy is best pony.

[2] 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 2×2 Latin square with the symbols $1, 2$ on the diagonal, i.e. $\begin{array}{|c|c|}\hline 1&\\\hline &2\\\hline\end{array}$, there's clearly no way to complete this to a Latin square.

Similarly, if we take a 3×3 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:

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

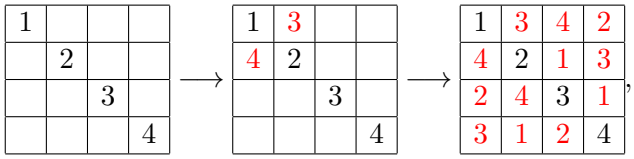
This square does not contain the symbols $1, 2, 3$ on its antidiagonal; therefore, there is no diagonal Latin square of order 3.

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 $(1, 2), (2, 1)$,

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

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



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?

Well: let's start smaller, and just ask that it's a normal Latin square. In order for this to hold, we need to not have any repeats in any given row: in other words, that no two cells $(i, j), (k, j)$ contain the same symbol. But this can happen only if

$$(ai + bj \equiv ak + bj \mod n) \Leftrightarrow (ai \equiv ak \mod n).$$

If a and n have common factors, then this is possible; let $i = 0$ and $k = \frac{n}{\text{GCD}(a,n)}$. However, if a and n are relatively prime, then this can only happen if $i = k$; i.e. if we've picked the same cell! So we have no repeats in any row if and ony if a and n are relatively prime.

Similarly, if we look at any column, we can see that there are no repeats in any column if and only if b and n are relatively prime. Therefore, this construction is a Latin square if and only if a, b are both relatively prime to n.

What about being a diagonal Latin square? Well: to insure this, we also need that the main diagonal and main antidiagonal have no repeats. However, the main diagonal is just

0				
	$b+a$			
		$2(b+a)$		
			$\ddots$	
				$(n-1)(b+a)$

,

i.e. the sequence made by looking at multiples of $(a+b)$. This clearly has no repeats if and only if $(a+b)$ is relatively prime to n. Similarly, the main antidiagonal has the form

					$(n-1)(a)$
				$b+(n-2)a$	
			$\iddots$		
		$(n-3)b+2a$			
	$(n-2)b+a$				
$(n-1)b$					

,

which, if we subtract nb from the entire main diagonal (which we can do, because we're just looking at everything mod n, and therefore nb is just 0) we can see is just

					$-b+(n-1)(a-b)$
				$-b+(n-2)(a-b)$	
			$\iddots$		
		$-b+2(a-b)$			
	$-b+(a-b)$				
$-b$					

,

Using the same logic as before, we can again see that this antidiagonal has no repeats if and only if $a-b$ is relatively prime to n.

By combining these observations, we have the following proposition:

Proposition. Suppose that n is an integer such that there are two numbers $a, b \in \{0, \ldots n-1\}$, such that $a, b, a+b, a-b$ are all relatively prime to n. Then the construction above creates a diagonal Latin square.

In particular, we have the following really easy corollary:

Corollary 1 *If n is an odd number that's not divisible by 3, there is a diagonal Latin square of order n.*

Proof. Set $a = 2, b = 1$; then $a, b, a+b = 3, a-b = 1$ are all relatively prime to n.

As an example, here's the result of our construction for $n = 5$:

0	2	4	1	3
1	3	0	2	4
2	4	1	3	0
3	0	2	4	1
4	1	3	0	2

.

Check: it works! Furthermore, any Latin square produced by this process has the following nice property:

Proposition. Given a Latin square L produced by the above process, the transpose[3] L^T is also a diagonal Latin square, and is furthermore orthogonal to L.

Proof. That L^T is diagonal is trivial: flipping a Latin square over a diagonal clearly doesn't change any of the properties involved in being a diagonal Latin square.

That L and L^T are orthogonal is only slightly harder. Take any pair of cells (i, j) and (x, y), and suppose that when we superimpose L on top of L^T, we see the same pair of symbols in each of those two cells.

Notice that by definition, L has the symbol $ai + bj$ in cell (i, j) and the symbol $ax + by$ in the cell (x, y). Similarly, because L^T is just formed by flipping L over its main diagonal, we have that the (i, j) cell of L^T is just the (j, i) cell of L, and therefore it contains the symbol $aj + bi$ (and as well that cell (x, y) contains $ay + bx$.)

Then, if we see the same pair of symbols in each of those two cells, we're claiming that

$$(ai + bj, aj + bi) \equiv (ax + by, ay + bx) \mod n$$

This is equivalent to the pair of equations

$$ai + bj \equiv ax + by \mod n, \quad aj + bi \equiv ay + bx \mod n.$$

By adding these two equations together, we get

$$\begin{aligned} &a(i + j) + b(i + j) \equiv a(x + y) + b(x + y) \mod n \\ \Rightarrow &(a + b)(i + j) \equiv (a + b)(x + y) \mod n, \end{aligned}$$

which (by dividing through by $a + b$, which we can do because $a + b$ is relatively prime to n) gives us $a + b \equiv x + y \mod n$.

Similarly, if we take the difference of those two equations, we also get

$$\begin{aligned} &a(i - j) - b(i - j) \equiv a(x - y) - b(x - y) \mod n \\ \Rightarrow &(a - b)(i - j) \equiv (a - b)(x - y) \mod n, \end{aligned}$$

which (by dividing through by $a - b$, which we can do because $a - b$ is relatively prime to n) gives us $a - b \equiv x - y \mod n$.

Adding these two equations gives us $2a \equiv 2x \mod n$; because n is odd, this tells us $a = x$. This in turn gives us $b = y$, and therefore that these two cells are the same!

Therefore, we have just shown that there are no repeated pairs of symbols when these two squares are superimposed; therefore, they are orthogonal.

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

Why do we care? Well: we started by talking about magic squares. As it turns out, we can turn a pair of these orthogonal diagonal Latin squares into a Magic square with no effort at all:

Proposition. Given any pair of orthogonal diagonal Latin squares L_1, L_2 on the symbols $\{0, \dots n-1\}$, we can create a magic square.

Proof. Take L_1 and superimpose it on L_2. Use this to create a magic square M as follows: if the cell (i, j) contains the ordered pair of symbols (x, y) in $L_1 + L_2$, write down the number $nx + y$ in the cell (i, j) of M.

Because we have every possible pair of symbols (r, s), we will get every possible number in $\{0, \dots n^2 - 1\}$ as an entry in our square, because any number a from this interval can be expressed in the form $r \cdot n + s$ (let s be its remainder when divided by n, and r be $\lfloor a/n \rfloor$.)

As well, consider the sum of all of the elements in any row. Because every symbol $r \in \{0 \dots n-1\}$ shows up in any row of L_1 exacty once, and similarly every symbol $s \in \{0 \dots n-1\}$ shows up in any row of L_2 exactly once, we have that

$$\sum_{\text{row of } M} = n \cdot \sum_{r=0}^{n-1} r + \sum_{s=0}^{n-1} s = n \cdot \left(\frac{n(n-1)}{2} \right) + \frac{n(n-1)}{2} = \frac{(n+1)(n)(n-1)}{2}.$$

But the only property we used to deduce this sum was the observation that in this row, every symbol r and s occured exactly once! This observation holds true for every column and the two diagonals, as well: therefore, these all have the same sums (in particular, $\frac{(n+1)(n)(n-1)}{2}$.) Therefore, our square is magic!

To illustrate how this works, here's a pair of orthogonal diagonal Latin squares, along with their resulting magic square:

0	2	4	1	3
1	3	0	2	4
2	4	1	3	0
3	0	2	4	1
4	1	3	0	2

,

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

$\longrightarrow$

(0,0)	(2,1)	(4,2)	(1,3)	(3,4)
(1,2)	(3,3)	(0,4)	(2,0)	(4,1)
(2,4)	(4,0)	(1,1)	(3,2)	(0,3)
(3,1)	(0,2)	(2,3)	(4,4)	(1,0)
(4,3)	(1,4)	(3,0)	(0,1)	(2,2)

$\equiv$

0	11	22	8	19
7	18	4	10	21
14	20	7	17	3
16	2	13	24	5
23	9	15	1	12

.