Math 7H Professor: Padraic Bartlett

Lecture 9: Latin Squares and Geometry

Week 9 *UCSB*

At the end of our last class, we gave an a brief introduction to an object that I spent the bulk of my Ph.D studying: **Latin squares**!

Definition. A **Latin square** of order n is a $n \times n$ array filled with n distinct symbols (by convention $\{1, \ldots n\}$), such that no symbol is repeated twice in any row or column.

Example. Here are all of the Latin squares of order 2:

1	2
2	1

2	1
1	2

.

A quick observation we should make is the following:

Proposition. Latin squares exist for all n.

Proof. Behold!

1	2	$\ldots$	$n-1$	n
2	3	$\ldots$	n	1
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
n	1	$\ldots$	$n-2$	$n-1$

□

Given this observation, a natural question to ask might be "How many Latin squares exist of a given order n?" And indeed, this is an excellent question! So excellent, in fact, that it turns out that we have no idea what the answer to it is; indeed, we only know the true number of Latin squares of any given order up to 11.

n	reduced Latin squares of size n[1]	all Latin squares of size n
1	1	1
2	1	2
3	1	12
4	4	576
5	56	161280
6	9408	812851200
7	16942080	61479419904000
8	535281401856	108776032459082956800
9	377597570964258816	5524751496156892842531225600
10	7580721483160132811489280	9982437658213039871725064756920320000
11	5363937773277371298119673540771840	776966836171770144107444346734230682311065600000
12	?	?

Asymptotically, the best we know (and you could show, given a lot of linear algebra tools) that

$$L(n) \sim \left(\frac{n}{e^2}\right)^{n^2}.$$

0.1 Mutually Orthogonal Latin Squares

In these notes, we look at a specific notion related to Latin squares — the concept of "orthogonal" Latin squares! To understand how this works, try solving the following problem:

Question. Take a deck of playing cards, and remove the 16 aces, kings, queens, and jacks from the deck. Can you arrange these cards into a 4 × 4 array, so that in each column and row, no two cards share the same suit or same face value?

This question should feel similar to the problem of constructing a Latin square: we have an array, and we want to fill it with symbols that are not repeated in any row or column. However, we have the additional constraint that we're actually putting **two** symbols in every cell: one corresponding to a suit, and another corresponding to a face value.

So: if we just look at the face values, we should get a 4 × 4 Latin square. Similarly, if we ignore the face values and look only at the suits, we should have a different 4 × 4 Latin square; as well, these two Latin squares ought to have the property that when we superimpose them (i.e. place one on top of the other), each of the resulting possible 16 pairs of symbols occurs exactly once (because we started with 16 distinct cards.)

You can do this! Here is one possible solution:

$A\heartsuit$	$K\diamondsuit$	$Q\spadesuit$	$J\clubsuit$
$K\spadesuit$	$A\clubsuit$	$J\heartsuit$	$Q\diamondsuit$
$Q\clubsuit$	$J\spadesuit$	$A\diamondsuit$	$K\heartsuit$
$J\diamondsuit$	$Q\heartsuit$	$K\clubsuit$	$A\spadesuit$

The generalization of this idea is to the concept of **orthogonality**[2] for Latin squares, which we define here:

Definition. A pair of $n \times n$ Latin squares are called **orthogonal** if when we superimpose them (i.e. place one on top of the other), each of the possible n^2 ordered pairs of symbols occur exactly once.

A collection of k $n \times n$ Latin squares is called **mutually orthogonal** if every pair of Latin squares in our collection is orthogonal.

[1] A **reduced** Latin square of size n is a Latin square where the first column and row are both $(1, 2, 3 \ldots n)$. The idea here is that by permuting the rows and columns of any Latin square, you can make it have this "reduced" property. Therefore, in a sense, the only interesting things to count are the number of different reduced squares; this is because from there you can generate any other Latin square by permuting its rows and columns.

[2] This idea has no obvious corresponding geometric context; just think of it as a name for now.

Example. The grid of playing cards we constructed earlier is a pair of 4×4 squares, for the reasons we discussed earlier. To further illustrate the idea, we present a pair of orthogonal 3×3 Latin squares:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

Like always, whenever we introduce a mathematical concept in combinatorics, our first instinct should be to attempt to count it! In other words: given an order n, what is the largest collection of mutually orthogonal Latin squares we can find? An upper bound is not too hard to find:

Proposition. For any n, the maximum size of a set of $n \times n$ mutually orthogonal Latin squares is $n-1$.

Proof. Take any collection $T_1, \ldots T_k$ of mutually orthogonal Latin squares. Then notice the following property: if we take any of our Latin squares and permute its symbols (i.e. switch all the 1 and 2's), the new square is still mutually orthogonal to all of the other squares. (Think about this for a bit if you are unpersuaded.)

Using the above observation, notice that we can without any loss of generality assume that the first row of each of our Latin squares is $(1, 2, 3 \ldots n)$. Now, take any pair of mutually orthogonal Latin squares from our collection, and look at the symbol in the cell in the first column/second row (i.e. the symbol at $(2, 1)$):

$$\begin{bmatrix} 1 & 2 & \ldots & n \\ x & - & \ldots & \\ \vdots & & & \\ - & - & \ldots & - \end{bmatrix}, \begin{bmatrix} 1 & 2 & \ldots & n \\ y & - & \ldots & \\ \vdots & & & \\ - & - & \ldots & - \end{bmatrix}.$$

We know that neither x nor y can be 1, because both of these squares are Latin squares. As well, we know that they cannot agree, as the first row of the superimposition of these two squares contains the pairs (k, k) , for every $1 \leq k \leq n$. This means that there are at most $n-1$ squares in our collection $T_1, \ldots T_k$, because there are $n-1$ distinct choices for the cell $(2, 1)$ that are not 1. □

We already know that sometimes $n-1$ is attainable: in our example above, we found 2 orthogonal Latin squares of order 3. When can we attain this bound?

This (somewhat frustratingly) turns out to be open! That is; we do not know for what values of n this bound is attainable.

However, there are some values of n for which we can answer this question: primes! To do this, we need to use the concept of **modular arithmetic**:

0.2 Modular arithmetic.

Definition. The set $\mathcal{C}$, of "clock numbers," is defined along with an addition operation $+$ and multiplication operation $\cdot$ as follows:

- Our set is the numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.
- Our addition operation is the operation "addition mod 12," or "clock arithmetic," defined as follows: we say that $a + b \equiv c \mod 12$ if the two integers $a + b$ and c differ by a multiple of 12. Another way of thinking of this is as follows: take a clock, and replace the 12 with a 0. To find out what the quantity $a + b$ is, take your clock, set the hour hand so that it points at a, and then advance the clock b hours; the result is what we call $a + b$.

  For example, $3 + 5 \equiv 8 \mod 12$, and $11 + 3 \equiv 2 \mod 12$. This operation tells us how to add things in our set.
- Similarly, our multiplication operation is the operation "multiplication mod 12," written $a \cdot b \equiv c \mod 12$, and holds whenever $a + b$ and c differ by a multiple of 12. Again, given any pair of numbers a, b, to find the result of this "clock multiplication," look at the integer $a \cdot b$, and add or take away copies of 12 until you get a number between 0 and 11.

  For example, $2 \cdot 3 \equiv 6 \mod 12$, $4 \cdot 4 \equiv 4 \mod 12$, and $6 \cdot 4 \equiv 0 \mod 12$.

We often will denote this object as $\langle \mathbb{Z}/12\mathbb{Z}, +, \cdot\rangle$, instead of as $\mathcal{C}$.

We can generalize this to the concept of **modular arithmetic**:

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot\rangle$ is defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n - 1\}$.
- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \equiv c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

On the HW, you are asked to prove the following claims:

Claim. Suppose that n is a **prime**[3] number[4]. Then $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot\rangle$ has the following property:

For any $a, b \in \{0, \ldots n - 1\}$, if $a \cdot b \equiv 0 \mod n$, then at least one of a, b are equal to 0.

Claim. Suppose that n is a prime. Take any $a \in \mathbb{Z}/n\mathbb{Z}$. If $a \neq 0$. then there is some $b \in \mathbb{Z}/n\mathbb{Z}$ such that $a \cdot b = 1$.

[3] A natural number n is called **prime** if it has the following property: for any pair of natural numbers a, b such that $a \cdot b = n$, exactly one of a, b is equal to 1. In other words, the only factors of n are 1 and itself, if you know what the word factor means. Notice that this means that 1 is not prime!

[4] Number systems! The positive whole numbers, $\{1, 2, 3, \ldots\}$, are called the **natural numbers**, and denoted via the symbol $\mathbb{N}$. Some mathematicians put 0 in their natural numbers; others do not. It's not very consistent. Similarly, the set of all whole numbers $\{\ldots - 2, -1, 0, 1, 2, \ldots\}$ is called the **integers**, and is denoted by the symbol $\mathbb{Z}$. (The $\mathbb{Z}$ comes from the German word for "numbers," *zahlen.*)

For example, in $\mathbb{Z}/5\mathbb{Z}$, we have that $2 \cdot 3 \equiv 1 \mod 5$, $3 \cdot 2 \equiv 1 \mod 5$, and $4 \cdot 4 \equiv 1 \mod 5$; so every element $a \in \mathbb{Z}/5\mathbb{Z}$ has some matched element b such that $a \cdot b = 1$!

We use it here to prove our claim about when mutually orthogonal Latin squares exist:

Proposition. Let p be a prime. Then there is a collection of $p-1$ mutually orthogonal Latin squares.

Proof. Notice the following fact: for any nonzero $a \in \mathbb{Z}/p\mathbb{Z}$, the grid=

$$\begin{bmatrix} a\cdot 0+0 & a\cdot 1+0 & \dots & a\cdot(n-1)+0 \\ a\cdot 0+1 & a\cdot 1+1 & \dots & a\cdot(n-1)+1 \\ \vdots & \vdots & \ddots & \vdots \\ a\cdot 0+(n-1) & a\cdot 1+(n-1) & \dots & a\cdot(n-1)+(n-1) \end{bmatrix},$$

where we've filled the cell (i,j) with the symbol $a \cdot i + j \in \mathbb{Z}/p\mathbb{Z}$, is a Latin square! To see why, suppose that there is some row i along which two cells (i,j) and (i,k) of this grid are the same. Then we have

$$\begin{aligned} a\cdot i + j = a \cdot i + k \mod p \\ \Rightarrow a\cdot i + j - (a\cdot i + k) \text{ is a multiple of } p \\ \Rightarrow j - k \text{ is a multiple of } p. \end{aligned}$$

But j, k are both values chosen from $\{0, 1, \dots p-1\} = \mathbb{Z}/p\mathbb{Z}$; therefore, the largest their difference can be is $p-1$, and the smallest it can be is $-(p-1)$. There is only one multiple of p in that span — namely, 0 — therefore, we must have $j - k = 0$. In other words, $j = k$! But this means that it is impossible for two **distinct** cells in our row to repeat a symbol, which is precisely one of the Latin properties!

Similarly, if we pick any column j along which two cells (i,j) and (k,j) of this grid are the same, we can do the same thing:

$$\begin{aligned} a\cdot i + j = a \cdot k + j \\ \Rightarrow a\cdot i + j - (a\cdot k + j) \text{ is a multiple of } p \\ \Rightarrow a \cdot (i-k) \text{ is a multiple of } p. \end{aligned}$$

We know that because $a \neq 0$, there is some element b such that $a \cdot b \equiv 1 \mod p$; consequently, the statement

$$a \cdot (i-k) \equiv 0 \mod p$$

is equivalent to the statement

$$b \cdot a \cdot (i-k) \equiv b \cdot 0 \mod p.$$

Because $b \cdot a = 1$, we know that this is just

$$(i-k) \equiv 0 \mod p,$$

which we know forces $i = k$ by our earlier logic. Therefore, just like above, it is impossible for two **distinct** cells in our column to repeat a symbol. In other words, these squares are Latin!

We have proven the first half our claim: this process generates $n-1$ distinct Latin squares. Label them T_a, for every element $a \in F$. We claim that this is fact a set of mutually orthogonal Latin squares! To see why, take any two squares T_a, T_b, and suppose that there are two cells $(i, j), (k, l)$ at which superimposing our two Latin squares yields the same ordered pair of symbols: i.e. that

$$a \cdot i + j \equiv a \cdot k + l \mod p \text{ and } b \cdot i + j \equiv b \cdot k + l \mod p.$$

Taking the difference of these two equations yields

$$(a-b) \cdot i \equiv (a-b) \cdot k \mod p.$$

Because $a \neq b$, we have that $a - b$ is nonzero, and therefore that it has some corresponding element c we can multiply it by to get 1. Do this to the LHS and RHS above, to get

$$\begin{aligned} c \cdot (a-b) \cdot i &\equiv c \cdot (a-b) \cdot k \mod p \\ &\Rightarrow i = k. \end{aligned}$$

Plugging this into our earlier equations yields $j = l$, and therefore that these two cells are the same. Therefore, it is impossible for two distinct cells to exist at which any two of our squares give the same pairs of symbols; in other words, we have made a set of $n-1$ mutually orthogonal Latin squares! □