Winter 2018, Math 148: Week 5 Problem Set
Due: Wednesday, February 14th, 2018
Applications of Finite Fields

Discussion problems. The problems below should be completed in class.

(D1) *Linear algebra over finite fields.*

(a) Draw the 2-dimensional vector space $\mathbb{F}_5^2$. Indicate which points lie in the span of $(3, 2)$.

(b) Draw the 2-dimensional vector space $\mathbb{F}_4^2$. Remember: the elements of $\mathbb{F}_4$ look like polynomials in a variable z! Find a line that avoids the points $(0, 1)$, $(1, 0)$, and $(1, 1)$.

(c) What is the maximum number of parallel lines you can find in $\mathbb{F}_5^2$? What about in $\mathbb{F}_4^2$? What do you conjecture about the maximum number of parallel lines in $\mathbb{F}_q^2$?

(d) How many lines go through the origin in $\mathbb{F}_5^2$? What about in $\mathbb{F}_4^2$? What if we use a different intersection point instead of the origin? Conjecture a general formula.

(e) Find a sequence $\{0\} \subsetneq A_1 \subsetneq A_2 \subsetneq \mathbb{F}_5^3$ of linear subspaces of $\mathbb{F}_5^3$. Are there longer sequences of linear subspaces in $\mathbb{F}_5^3$?

(f) Find the longest sequence $\{0\} \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq \mathbb{Z}_4^2$ of linear subspaces of $\mathbb{Z}_4^2$. What does this tell you about "dimension" over $\mathbb{Z}_4$? Note that $\mathbb{Z}_4$ has zero-divisors!

(g) How many 2-dimensional linear subspaces does $\mathbb{F}_5^3$ have? Conjecture a formula for the number of 2-dimensional subspaces of $\mathbb{F}_q^d$. What about k-dimensional subspaces?

(D2) *Latin squares.* Recall that a *latin square* of order n is an $n \times n$ grid filled with values $1, \ldots, n$ (or any set of n symbols) such that no entry is duplicated in any row and column. Recall further that two latin squares A and B of order n are *mutually orthogonal* if each pair (A_{ij}, B_{ij}) for $i, j \leq n$ occurs exactly once.

(a) Compare within your group the latin squares you found in the preliminary problem. Is there a third latin square that is mutually orthogonal to each of your first two?

(b) Given below is the playing card example from Friday with two mutually orthogonal latin squares of order $n = 4$ (one using the symbols $\{\mathrm{A}, \mathrm{K}, \mathrm{Q}, \mathrm{J}\}$ and the other using the symbols $\{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$). Can you find a third latin square that is mutually orthogonal to *both* of these? (You may use any 4 symbols you wish)

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

(c) The following result tells us how to construct latin squares of order p^r for p prime.

Theorem. *For each nonzero $a \in \mathbb{F}_q$, the $q \times q$ grid with entries given by*

$$L_{i,j} = ai + j \qquad \textit{for} \qquad i, j \in \mathbb{F}_q$$

is a latin square of order q. Moreover, for distinct nonzero $a, a' \in \mathbb{F}_q$, the latin squares constructed above are mutually orthogonal.

Use the above theorem to construct 3 mutually orthogonal latin squares of order 5. Verify that your latin squares are in fact mutually orthogonal. *Without using the theorem*, find a fourth mutually orthogonal latin square. Can there be more than one?

(d) Using the theorem in part (c), find 3 mutually orthogonal latin squares of order $n = 4$.

(e) Attempt to construct a latin square of order $n = 4$ using the theorem in part (c) with $\mathbb{Z}_4$ in place of the finite field. What breaks?

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) (a) Draw the 2-dimensional vector space $\mathbb{F}_9^2$.

(b) In your drawing from part (a), indicate which points lie in the span of $(1, 2) \in \mathbb{F}_9^2$.

(c) In your drawing from part (a), identify the points on a line parallel to the one in part (b) (ideally using different colors, but at the very least with *some* distinguishing mark like a circle, double circle, or square around the point).

(d) In your drawing from part (a), identify the points on the line passing through the points $(1, z)$ and $(z + 1, 2z^2)$, again using a different color or symbol than above. At which point(s) does this line intersect the line from part (b)?

(R2) (a) Draw the 2-dimensional vector space $\mathbb{F}_8^2$.

(b) In your drawing from part (a), indicate which points lie in the span of $(z, z^2) \in \mathbb{F}_8^2$.

(c) In your drawing from part (a), identify the points on a line parallel to the one in part (b) (ideally using different colors, but at the very least with *some* distinguishing mark like a circle, double circle, or square around the point).

(R3) Suppose $\mathbb{Z}_6$ is used in place of the finite field in the theorem in part (c) of discussion problem (D2). Which of the 5 squares are actually latin squares? Of those that are in fact latin squares, are any two mutually orthogonal?

Optional problems. Optional problems are not required for submission, but bonus points will be awarded for a complete solution.

(O1) The goal of this problem is to prove that there are at most $n - 1$ mutually orthogonal latin squares of order n. We will use the symbols $\{1, \ldots, n\}$.

(a) Suppose A and B are mutually orthogonal latin squares. Explain why if you switch the locations of all 2's and 3's in A (i.e. replace every 2 entry with a 3 and every 3 entry with a 2), the resulting latin square A' is also mutually orthogonal to B.

(b) A latin square is said to be in *standard form* if the entries in the top row appear in order. Suppose A and B are mutually orthogonal latin squares, and suppose A' and B' are latin squares in standard form obtained from A and B respectively by swapping entries as described in part (a). Explain why A' and B' are mutually orthogonal.

(c) Prove that it is impossible to have latin squares $A_1, \ldots, A_n$ of order n in such a way that any two are mutually orthogonal.