MATH 540 HONORS LINEAR ALGEBRA SUMMER 2021
PROBLEM SET B

Due Monday May 24 at 11:59pm Eastern, submitted in Gradescope

1. Read the Introductions in the Discussions page on Canvas. Leave some responses.
2. Fill in the following table of powers of 2 in $\mathbb{F}_{13}$. I've started it for you.[1]

n	0	1	2	3	4	5	6	7	8	9	10	11
2^n	1	2	4									

More problems will be added on Thursday 5/20. Please re-download this problem set then.

[1]Notice how the nonzero elements of $\mathbb{F}_{13}$ appear, once each, all scrambled up in the bottom row of the table. In this situation, 2 is called a *primitive element* of $\mathbb{F}_{13}$. The problem of "unscrambling" the bottom row is known as the *discrete logarithm problem* and is understood to be computationally hard. The hardness of this unscrambling problem forms the basis for some public-key cryptography schemes, e.g., *Diffie-Hellman key exchange*, in which two people can establish a shared secret while communicating entirely in public. You can look all of this up online. It is amazing!