MAT 534 — HOMEWORK 1

DUE ON FRIDAY 17 JANUARY

Read Chapters 0–2. (You can skim most of Chapter 0.) Also, find the author's website and poke around a little bit. It is linked from the syllabus and the course web page.

1. (Chapter 0, #11) Let n and a be positive integers and let $d = \gcd(a,n)$. Show that the equation $ax = 1 \bmod n$ has a solution for x if and only if $d = 1$. (Hint: Use Theorem 0.2.)

2. (Chapter 1, #2) Write out a complete Cayley table for D_3. Is D_3 Abelian?

3. (Chapter 1, #13) Describe the symmetries of a nonsquare rectangle (a mattress, say). Construct the Cayley table. (Hint: a piece of cardboard is a very useful thing.)

4. (Chapter 2, #9) Show that $\{1,2,3\}$ under multiplication modulo 4 is not a group, but that $\{1,2,3,4\}$ under multiplication modulo 5 is a group.

5. (Chapter 2, #31) Prove that every Cayley table (of a finite group) is a *Latin square,* that is, each element of the group appears *exactly* once in each row and column. (Notice that "appears exactly once" means *two* things: no repeats, and also each element does appear.)

Also suggested, but not to hand in:

(A) (Chapter 0, #9) Let n be a fixed integer greater than 1. If $a \bmod n = a' \bmod n$ and $b \bmod n = b' \bmod n$, prove that $a+b$ and $a'+b'$ agree modulo n, and that ab and $a'b'$ agree modulo n.

(B) (Chapter 0, #20–21) Let $p_1, p_2, \ldots, p_n$ be primes. Show that $p_1 p_2 \cdots p_n + 1$ is divisible by none of these primes. Conclude that there exist infinitely many primes.

(C) (Chapter 1, #21) What group-theoretic property do the uppercase letters F, G, J, L, P, Q, R have that is not shared by the remaining uppercase letters in the alphabet?

(D) (Chapter 2, #48) Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group under matrix multiplication. (This is called the *Heisenberg group*, and is crucially related to the Heisenberg Uncertainty Principle.)