MATH 534 – HOMEWORK 2

(1) Write down the group tables for $(\mathbb{Z}/4, +_4)$ and $((\mathbb{Z}/5)^\times, \times_5)$. Are they related? If so, explain how.

(2) For each of the following groups G, find $|G|$ and $|g|$ for every $g \in G$ (be sure to show your work!):
  (a) $G = \mathbb{Z}/12$
  (b) $G = (\mathbb{Z}/12)^\times$
  (c) $G = (\mathbb{Z}/16)^\times$
  (d) $G =$ the group of symmetries of a square

(3) Recall from lecture that Wilson's Theorem states that a number n is prime if and only if $(n-1)! \equiv -1 \mod n$. We proved that n being prime implies the above congruence. In this problem, we'll complete the proof by showing that if n isn't prime, then $(n-1)! \not\equiv -1 \mod n$.

  (a) Complete (*i.e.* fill in the blank with the correct number) and then prove the following statement: if n is not prime and $n \neq$ ____, then $(n-1)! \equiv 0 \mod n$.

  (b) Prove the only thing left to prove to complete our proof of Wilson's Theorem.

  (Hint: there is no group theory involved in this problem. Think about what it means for a number to not be prime. You also may want to consider separately the case when n is the square of a prime number.)

(4) Let G be a group. The **center** of G is defined via:

$$\mathcal{Z}(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

  Prove the following: If $a \in G$ is the only element in G of order 2, then $a \in \mathcal{Z}(G)$.

  (Hint: what does it mean if a isn't in $\mathcal{Z}(G)$?)

  Note: next week, we'll define the notion of a subgroup, and $\mathcal{Z}(G)$ will be an example of a subgroup of G. After we've discussed the definition, convince yourself of this, either by proving it yourself (no need to turn this bit in), or by reading the proof in the book.