Homework 5 | **John Waczak**
MTH 343 | Date: November 5, 2017
Prof. Ren Guo

9.3.15

List all of the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Recall the definitions fo the following groups:

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$
$$\mathbb{Z}_2 = \{0, 1\}$$

Thus, we create $\mathbb{Z}_2 \times \mathbb{Z}_4$ via the Cartesian product of the two sets:

$$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\} \tag{1}$$

9.3.16.b

Find the order of $(6, 15, 4) \in \mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$.

Recall Corollary 9.18: For $(g_1...g_n) \in \Pi_i G_i$ if g_i has finite order r_i then the order of $(g_1...g_n)$ is the least common multiple of $r_1, ...r_n$.

So, we simply need to find the individual order of 6, 15, and 4 in order to determine the order of (6,15,4). Observe that:

$$\begin{aligned} 6 * 5 &\mod (30) = 0 \\ 15 * 3 &\mod (45) = 0 \\ 4 * 6 &\mod (24) = 0 \end{aligned}$$

So now that we have the order of each number in the tuple, the order of (6,15,4) is simply:

$$LCM(6, 15, 4) = 30 \tag{2}$$

Thus the order of (6, 15, 4) is 30 by Corollary 9.18. □

9.3.32

Prove that $U(5) \cong \mathbb{Z}_4$. *Can you generalize this for U(p) where p is prime?*

Recall that $U(5) = \{1, 2, 3, 4\}$ and $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. To prove that these two groups are isomorphic, we simply need to prove that U(5) is cyclic as both U(5) and $\mathbb{Z}_4$ have the same order (4).

$$\begin{aligned} 2 &\mod (5) = 2 \\ 2^2 &\mod (5) = 4 \\ 2^3 &\mod (5) = 8 \mod (5) = 3 \\ 2^4 &\mod (5) = 16 \mod (5) = 1 = e \end{aligned}$$

Thus 2 is a generator for U(5) and therefore U(5) is cyclic. U(5) is a cyclic group of order 4 and so by theorem 9.8, $U(5) \cong \mathbb{Z}_4$.

In order to extend this theorem to groups of the form $U(p)$ where p is prime, we need to be able to prove that $U(p)$ is cyclic so long a p is prime. First let's consider the type of elements in U(p). By definition this is all of the non-zero elements of $\mathbb{Z}_p$ that are relatively prime to p (i.e. k such that $gcd(k, p) = 1$). Since p itself is prime it's only divisors are 1 and itself. Thus U(p) is necessarily all of the integers from 1 up to p-1:

$$U(p) = \{1, 2, 3...p - 1\} \tag{3}$$

For U(p) to be cyclic, it remains to find a generator for U(p). While in most cases there are multiple generators, the only option that has a clear chance of being the generator for every p is the element (p-1). Fermat's Little Theorem (6.19) gives us that:

$$a^{p-1} \equiv 1 \mod (p) \tag{4}$$