PROBLEM N.4: INVERSES OF $\mathbb{Z}_m$

ROSIE KEY

1. Definitions

To first understand how to determine if an element of $\mathbb{Z}_m$ is an inverse of m, it is important to define what an inverse is. An inverse is a non-zero integer a such that when multiplied by another non-zero integer b,

$$a \cdot b = mk + 1$$

where k is some integer. In other words, it is two numbers a and b such that their product is a multiple of m plus one. Also, recall that the set of all residue classes is given by

$$\mathbb{Z}_m = 0, 1, 2, 3, 4, 5, ..., (m - 1).$$

2. Determining Inverses of $\mathbb{Z}_m$

Conjecture 1.) Consider the scenario where integer $a = b$ or

$$a^2 = mk + 1.$$

This means that if the sum of m and 1 has a square root, that root will be an inverse of m.

Conjecture 2.) Consider if m were to equal an odd number greater than one and the integer k was odd. This means that m plus one would be an even number, which would automatically make 2 an inverse.

Conjecture 3.) Consider $k = 0$. This means the following:

$$a \cdot b = m \cdot 0 + 1$$

$$a \cdot b = 1$$

$$a = b = 1$$

This means that for any m value greater than one, 1 will always be an inverse of m.

Date: March 2019.