Problem N.4

Inverses of $\mathbb{Z}_m$

Due Date: 3/25/2019
Folder: `NumberTheory`
File Name: `N4_Inverses_Name.py`
Points: 2 points

Learning Objectives

- Mix of programming skills

Problem Background

Recall the basics of modular arithmetic and the group $\mathbb{Z}_m$. We know that the set of all residue classes is given by,

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

Addition, subtraction and multiplication on these elements is done similarly to regular integers, but using modular arithmetic.

For example, assume we are considering $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. In $\mathbb{Z}_7$ we have that 5+4=2, because $9 \equiv 2 (mod\ 7)$. Also, $2 \cdot 4 = 1$, because $2 \cdot 7 = 8$ and $8 \equiv 1 (mod\ 7)$.

Many things are similar between $\mathbb{Z}_m$ and the integers, but some things are different. One of those things involves multiplicative inverses. A **multiplicative inverse** of an element a is an element b such that $a \cdot b = 1$. So for instance, about we saw that in $\mathbb{Z}_7$, when you multiple 2 and 4, they equal 1. Therefore, both 2 and 7 are inverses of each other in the set $\mathbb{Z}_7$. The key change in $\mathbb{Z}_m$ is that not all element have an inverse. The number of inverses and which elements have inverses will change depending on what the m is in $\mathbb{Z}_m$.

Program Criteria

Write a program that does the following:

- Create an input variable `m` that will represent which $\mathbb{Z}_m$ set we are working with.
- Determine which elements of $\mathbb{Z}_m$ are have a multiplicative inverse.
- Print out all the elements of $\mathbb{Z}_m$ that have a multiplicative inverse and how many such elements there are, with appropriate descriptive text.

Deliverables

Place the following in a folder named `NumberTheory` in your repository:

- A Python file `N4_Inverses_Name.py` that satisfies the program criteria.
- A pdf file `N4_Inverses_Name.pdf` describe a simple test for whether a particular element of $\mathbb{Z}_m$ has an inverse. This test will probably depend on m. This should not be a description of your program, but a simpler test that will describe all elements that have an inverse.