Problem N.7

Quadratic Residues

Due Date: 4/5/2019
Folder: `NumberTheory`
File Name: `N7_Quadratic_Name.py`
Points: 5 points

Learning Objectives

- Consider properties of quadratic residues

Problem Background

When considering elements of $\mathbb{Z}_p$, we define a quadratic residue to be the numbers $n \in \mathbb{Z}_p$ such that there exists a $k \in \mathbb{Z}_p$ where

$$n = k^2.$$

For example, let us consider $\mathbb{Z}_1 1$. Then 1 is an obvious quadratic residue, since $1 = 1^2$. However, 3 is also a quadratic residue of $\mathbb{Z}_1 1$, since $3 = 6^2 = 36 \equiv 3 (\text{mod}) 11$.

There are some interesting patterns that occur when we consider $\mathbb{Z}_p$ where p is prime. Therefore, for this problem we assume that p is prime for each of our $\mathbb{Z}_p$. We will consider two questions. First, how many elements of $\mathbb{Z}_p$ are quadratic residues. The second question we consider is what values for p makes -1 a quadratic residue. Recall that -1 = (p-1) in $\mathbb{Z}_p$.

Program Criteria

Write a program that does the following:

- Create a variable `P` to denote the maximum value for p in your code.
- Counts the number of quadratic residues in $\mathbb{Z}_p$.
  - ⋆ Create a 2D numpy array `count` to store your results. This array will have 2 columns:

p	Number of quadratic residues in $\mathbb{Z}_p$

    The first column stores the value for p, the second column stores the number of quadratic residues in $\mathbb{Z}_p$.
  - ⋆ For all primes $p \leq P$, count the number of quadratic residues in $\mathbb{Z}_p$ and store the number in the `count` array.
  - ⋆ Print out `count` with appropriate text.
- Check if $-1 \in \mathbb{Z}_p$ is a quadratic residue
  - ⋆ Create a 2D numpy array `neg_one` to store your results. This array will have 2 columns:

p	Is -1 quadratic residue?

    The first column stores the value for p, the second column stores a `True` or `False` values, with `True` representing that -1 is a quadratic residue, and `False` stating otherwise.
  - ⋆ For all primes $p \leq P$, determine if $-1 \in \mathbb{Z}_p$ is a quadratic residue of $\mathbb{Z}_p$ and store the result in the `neg_one` array.
  - ⋆ Print out `neg_one` with appropriate text.

Deliverables

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

- A Python file `N7_Quadratic_Name.py` that satisfies the program criteria.
- A pdf file `N7_Quadratic_Name.pdf` created with Latex:
  - ⋆ State any patterns you notice relating the number of quadratic residues in $\mathbb{Z}_p$ to the value of p.
  - ⋆ State any patterns you notices relating whether $-1 \in \mathbb{Z}_p$ is a quadratic residue to the value of p.