Math Circles - Elementary Number Theory - Fall 2023

Exercises

Introduction

1. Compute $3^{894} \mod 9$.
2. Compute the last digit of 7^{82}.

Fermat's Little Theorem

1. Prove that if p is prime and $1 \leq a \leq p-1$, then $a^{k(p-1)} \equiv 1 \mod p$ for all integers k.
2. Compute $4^{42} \mod 7$.
3. If p is prime, is it ever possible for there to be an integer $a \in \{2, \ldots, p-1\}$ such that $a^i = 1$ for some $1 \leq i < p-1$? Either find an example of a and p for which this is true, or prove that for all choices of a and p, $a^i \neq 1 \mod p$ for all $1 \leq i < p-1$.

Euler's Totient Theorem

1. Prove that if $\gcd(a, n) = 1$, then $a^{k(\Phi(n))} \equiv 1 \mod n$ for all integers k.
2. Compute $11^{48} \mod 35$.
3. Find the last two digits of $7^{81} - 3^{81}$.

HARD EXERCISES

1. Prove Wilson's Theorem: An integer p is prime if and only if $(p-1)! \equiv p-1 \mod p$.