Math 11N
Homework 5
Due Saturday, February 12th, 2022

1. (Computations) Do each of the following computations below. Show your work, don't just write the answer!

   (a) Reduce $84526 \cdot 862967^3 - 448184 \cdot 591183^2 \bmod 15$.

   (b) Compute $1477^{-1} \bmod 9235$.

   (c) Reduce $1769^{234} \bmod 31$.

   (d) Reduce $1! + 2! + \ldots + 100! \bmod 25$.

2. Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for all $n \in \mathbb{Z}$.

3. This problem deals with divisibility tests for integers. Let $n = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$ be the decimal expansion of n. For example, $123 = 1 \cdot 100 + 2 \cdot 10 + 3$.

   (a) Prove that n is divisible by 3 if and only if $a_0 + a_1 + \ldots + a_n$ is divisible by 3. Show that a similar condition holds for divisibility by 9, but does not work for divisibility by 27.

   (b) Prove that n is divisible by 11 if and only if $a_0 - a_1 + a_2 + \ldots + (-1)^n a_n$ is divisible by 11.

   (c) For $k \geq 1$, prove that n is divisible by 2^k if and only if the last k digits of n are divisible by 2^k. Show that a similar condition holds for powers of 5 as well.

4. This problem deals with solving linear equations in $\mathbb{Z}/n\mathbb{Z}$, which we know is the same as solving linear congruences mod n. Assume $n > 1$ is an integer, and that a, b are integers.

   (a) Show that the congruence $ax \equiv b \bmod n$ is solvable if and only if $\gcd(a, n) \mid b$.

   (b) If x_0 is a solution to $ax \equiv b \bmod n$, prove that all the solutions to $[a]x = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ are $[x_0 + \frac{n}{\gcd(a,n)}k]$ for $k = 0, 1, \ldots, (a, n) - 1$. *(Remember: $[x]$ denotes the congruence class of x mod n, and that the elements of $\mathbb{Z}/n\mathbb{Z}$ are congruence classes, not numbers!)*

   (c) Solve the congruences $1723x \equiv 3574 \bmod 4914$ and $126x \equiv 91 \bmod 217$. Your answer should be a single congruence class in each case: $x \equiv \_ \bmod \_$.

   (d) Write down the solutions to $[1723]x = [3574]$ in $\mathbb{Z}/4914\mathbb{Z}$ and $[126]x = [91]$ in $\mathbb{Z}/217\mathbb{Z}$.

   In particular, this problems shows that it's possible for a linear equation in $\mathbb{Z}/n\mathbb{Z}$ to have more than one solution in $\mathbb{Z}/n\mathbb{Z}$, which is very different from how things work in $\mathbb{Z}$!

5. The goal of this problem is to demonstrate how working in $\mathbb{Z}/n\mathbb{Z}$ can detect obstruction to equations having integer solutions.

   (a) Write down the perfect squares in $\mathbb{Z}/8\mathbb{Z}$ and perfect cubes in $\mathbb{Z}/9\mathbb{Z}$.

   (b) Prove that $x^3 + y^3 + z^3 = 4$ has no integer solutions. For what other integers can you replace 4 with and have your same argument work?

   (c) Prove that there are no integers m, n such that $3^m + 3^n + 1$ is a perfect square.

6. (a) Prove that if p is prime, then $(p-1)! \equiv -1 \bmod p$ *(Hint: try pairing up integers in the product in a useful way)*.

   (b) Prove that if $n > 4$ is composite, then $(n-1)! \equiv 0 \bmod n$.

   Combining these two parts says than an integer is prime if and only if $n \nmid (n-1)!$. Of course, this is a very *bad* way of checking that an integer is prime, because $(n-1)!$ gets very large, very fast!