# Homework 4

*Due: Wednesday, February 26*

All homeworks are due at 12:55 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

## Problem 1

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Let $n \in \mathbb{Z}^+$. Prove the following statements:

a. $ac \equiv bd \pmod{m}$.

b. $a^n \equiv b^n \pmod{m}$.

   **Hint**: Try induction on $n$.

## Problem 2

a. Find the values of $x$ that satisfy each congruence. If there are infinitely many, list four of them and state the pattern.

   i. $x \equiv 5 \pmod{6}$
   ii. $x \equiv -8 \pmod{6}$
   iii. $x \equiv 12 \pmod{1}$
   iv. $x^2 \equiv 1 \pmod{8}$
   v. $6 \equiv 12 \pmod{x}$

b. Compute the greatest common divisor of the numbers specified using the Euclidean algorithm. Furthermore, for each pair, express the gcd as a linear combination of the given numbers. Show all steps.

   i. $16, 23$
   ii. $20, 72$

c. Use the Euclidean algorithm to find $x$. Show all steps.

   i. $3x \equiv 1 \pmod{11}$
   ii. $7x \equiv 3 \pmod{19}$

## Problem 3

Given that $x$ and $y$ are integers, prove that $11|2x + 3y$ if and only if $11|10x + 4y$.

## Problem 4

a. Beret and Cueball live in a world with an infinite number of 314 donut boxes and 159 donut boxes, meaning that in this world, whenever you want a 314 donut box or a 159 donut box you can instantly have one. Prove that they can exchange any amount of donuts—for example, a customer can give them 155 donuts by giving them a 314 donut box, and receiving a 159 donut box.

b. Beret and Cueball step through the rabbit hole into a different world. In this world, they can have an infinite amount of donuts with denominations $p$ (a prime) and $(p-1)(p+1)$. Prove that they can still exchange any amount of donuts. (The donuts cannot be seperated from their boxes).

## Problem 5

Let $A_n$ denote the set of integers between 0 and $n-1$, inclusive, which are relatively prime to $n$. Prove by constructing a bijection that if $n$ is odd, $|A_n| = |A_{2n}|$.