

ASSIGNMENT-2
CS 2214: DISCRETE STRUCTURES FOR COMPUTING
DUE FEBRUARY 13 TH 2020, 11:55 PM

Instructions: Please submit a **single pdf file** in gradescope.

1. (25 points) Let p be a prime number and a an integer not divisible by p . Prove that there exists an integer b such that $ab \equiv 1 \pmod{p}$. Conclude that every non-zero element in \mathbb{Z}_p has a multiplicative inverse.

Hint: Use Bezout's identity.

2. (25 points) Let x be an integer such that x leaves a remainder 3 when divided by 5, leaves a remainder 7 when divided by 12 and it leaves a remainder 8 when divided by 13. Find the remainder when you divide x by 780 using the Euclidean algorithm.

Hint: Chinese remainder theorem and the example following it in textbook.

3. (25 points) Let n be a positive integer. Prove that if $2^n - 1$ is a prime number then n is a prime number.

4. (25 points) Prove that there does not exist integers any a and b such that the function $p(n) = n^2 + an + b$ is a prime number for every positive integer n .

Hint: First prove that if such a polynomial exists then $b = 1$. Then use modular arithmetic to conclude the result.