COMP 2711 Discrete Math Tools for Computer Science

2022 Fall Semester - Homework 4

Question 1: Answer the questions below:

(a) Find all positive integers n such that $n^2 + 1$is divisible by $n + 1$.

(b) Find all integers $x \neq 1$ such that $x - 1 \mid x^3 - 3$.

(c) Prove that if for integers a and b we have $7 \mid a^2 + b^2$, then $7 \mid a$ and $7 \mid b$

(d) Prove that if for some integers a, b, c, we have $9 \mid a^3 + b^3 + c^3$, then at least one of the numbers a, b, c is divisible by 3.

(e) Prove that if for integer a and b the congruence $ax + b = 0 (\text{mod } m)$ has a solution for every positive integer modulus m, then the equation $ax + b = 0$ has an integer solution.

Question 2: Solve each of these congruences. Please write down the process of finding multiplicative inverses. If you just write down the answer, you will get 0 point even if the answer is correct.

(a) $2011x \equiv 123 (\text{mod } 2711)$

(b) $3675x \equiv 291 (\text{mod } 4409)$

(c) $777x \equiv 896 (\text{mod } 2311)$

Question 3: Solve this system of linear congruences. If you just write down the answer, you will get 0 point even if the answer is correct.

$$x \equiv 2 (\text{mod } 7)$$
$$x \equiv 3 (\text{mod } 17)$$
$$x \equiv 15 (\text{mod } 23)$$
$$x \equiv 14 (\text{mod } 27)$$

Question 4: Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$

(ii) Bob's private key is $d = e^{-1} \bmod (n - 1)$.

(iii) Alice encrypts a message $m (0 < m < n - 1)$ by calculating $c = m^e \bmod n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \bmod n$.

Suppose $n = 251$ and $e = 137$.

(a) Calculate d using the extended GCD algorithm. Show the computational steps.

(b) Suppose $m = 200$. Calculate $c = m^e \bmod n$ using repeated squaring. Show the computational steps.

(c) Is the system secure? Explain why or why not.