CSE 311: Foundations of Computing I

Section 5: Number Theory and Induction

1. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Find the multiplicative inverse of 6 modulo 7.

(d) Does 49 have an multiplicative inverse modulo 7?

2. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2(\text{mod } 33)$ for all of its integer solutions z.

3. Induction

(a) For any $n \in \mathbb{N}$, define S_n to be the sum of the squares of the first n positive integers, or

$$S_n = 1^2 + 2^2 + \cdots + n^2.$$

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

(b) Define the triangle numbers as $\triangle_n = 1+2+\cdots+n$, where $n \in \mathbb{N}$. We showed in lecture that $\triangle_n = \frac{n(n+1)}{2}$. Prove the following equality for all $n \in \mathbb{N}$:

$$0^3 + 1^3 + \cdots + n^3 = \triangle_n^2$$

(c) Prove for all $n \in \mathbb{N}$ that if you have two groups of numbers, $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$, such that $\forall (i \in [n]).\ a_i \leq b_i$, then it must be that:

$$a_1 + \cdots + a_n \leq b_1 + \cdots + b_n$$

4. Casting Out Nines

(a) Suppose that $a \equiv b$ (mod m). Prove by induction that for every integer $n \geq 1$, $a^n \equiv b^n$ (mod m).

(b) Let $K \in \mathbb{N}$. Prove that if $K \equiv 0$ (mod 9), then the sum of the digits of K is a multiple of 9.