CSE 311: Foundations of Computing I

Section 5: Number Theory

1. Casting Out Nines

Let $n \in \mathbb{N}$. Prove that if $n \equiv 0 \pmod 9$, then the sum of the digits of n is a multiple of 9.
You may use without proof that $a \equiv b \pmod m \rightarrow a^i \equiv b^i \pmod m$.

2. 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?

(e) Find the multiplicative inverse of 7 modulo 311.

(f) Find the multiplicative inverse of 27 modulo 151.

3. 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 $7z \equiv 2 \pmod{33}$.

4. Modular Exponentiation

Compute $7^{18} \bmod 23$ using the efficient modular exponentation algorithm. Show your intermediate results.

5. More Number Theory

(a) Prove that if $n^2 + 1$ is a perfect square, where n is an integer, then n is even.

(b) Prove that if n is a positive integer such that the sum of the divisors of n is $n + 1$, then n is prime.