CS201: Discrete Math for Computer Science
2024 Spring Semester Written Assignment
#3 Due: Apr. 2th, 2025

The assignment needs to be written in English. Assignments in any other language will get zero point. Any plagiarism behavior will lead to zero point.

Q. 1. Show that if a | b and b | a, where a and b are integers, then a = b or *a = −b.*

Q. 2. Let a, b, and c be integers. Suppose m is an integer greater than 1 and ac ≡ bc (mod m). Prove a ≡ b (mod m/ gcd(c, m)).

Q. 3. For two integers a, b, suppose that gcd(a, b) = 1 and b ≥ a. Prove that gcd(b + a, b − a) ≤ 2.

Q. 4. Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if an−1 ≡ 1 (mod n).

(a) For a = 2, does n = 561 pass the test?

(b) Did the test give the correct answer in this case?

Q. 5. Solve the following linear congruence equations.

(a) 778x ≡ 10 (mod 379).

(b) 312x ≡ 3 (mod 97).

Q. 6. Find all solutions, if any, to the system of congruences x ≡ 5 (mod 6), *x ≡ 3 (mod 10), and x ≡ 8 (mod 15).*

Q. 7. Prove that if a and m are positive integer such that gcd(a, m) = 1 then the function

$$f : \{0, . . . , m - 1\} \rightarrow \{0, . . . , m - 1\}$$

defined by

$$f(x) = (a \cdot x) \bmod m$$

is a bijection.

Q. 8. Let m1, m2, . . . , mn be pairwise relatively prime integers greater than or equal to 2. Show that if a ≡ b (mod mi) for i = 1, 2, . . . , n, then a ≡ b (mod m), where m = m1m2 · · · mn.

Q. 9. Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of (p − 1)(q − 1).