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 $a \mid b$ and $b \mid a$, 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 $ac \equiv bc \pmod{m}$. Prove $a \equiv b \pmod{m/\gcd(c, m)}$.

Q. 3. For two integers a, b, suppose that $\gcd(a, b) = 1$ and $b \geq a$. Prove that $\gcd(b + a, b - a) \leq 2$.

Q. 4. Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

(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) $778x \equiv 10 \pmod{379}$.

(b) $312x \equiv 3 \pmod{97}$.

Q. 6. Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

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

$$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$$

defined by

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

is a bijection.

Q. 8. Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1 m_2 \cdots m_n$.

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 $(p-1)(q-1)$.