Name:
Student ID:

CSED261: Discrete Mathematics for Computer Science
Homework 5: Number Theory and Cryptography

Question 1. Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with $m \geq 2$, then $a - c \equiv b - d \pmod{m}$.

Solutions

Question 2. Show that a positive integer is divisible by 11 if and only if the difference of the sum of its decimal digits in even-numbered positions and the sum of its decimal digits in odd-numbered positions is divisible by 11.

Solutions

Question 3. Use the Euclidean algorithm to find

(a) gcd(1, 5)

(b) gcd(100, 101)

(c) gcd(123, 277)

(d) gcd(1529, 14039)

(e) gcd(1529, 14038)

(f) gcd(11111, 111111)

Solutions

Question 4. Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a,m) = \gcd(b,m)$.

Solutions

Question 5. Solve the system of congruence $x \equiv 3 \pmod{6}$ and $x \equiv 4 \pmod{7}$ using the method of back substitution.

Solutions

Question 6. Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

Solutions