DEPARTMENT OF COMPUTER SCIENCE

CSC2901 – Discrete Structures

Test I

Instructions : Answer **ALL** the questions

Duration : 2 Hours

---

1. Prove that
   a. If the sum of two integers is even, so is their difference.
   b. If $a \equiv b(mod\ n)$ then $ac \equiv bc(mod\ n)$, for integers a, b, c, and n

2.
   a. For the pair of integers a and b below, find the numbers m and n, if possible, such that $am + bn = 1$.
      i. $a = 10, b = 7$
      ii. $a = 10, b = 8$

   b. What condition should exist between a and b, for numbers m and n to be found such that $am + bn = 1$?
   c. Find the number s such that $7s \equiv 1(mod\ 24)$

3. Ben intends to communicate with Ann securely using the RSA algorithm. So he picks the primes $p = 13$ and $q = 5$
   a. What public key does he send to Ann?
   b. Ben receives the message "F", encoded by Ann. What is the plaintext of this message?

4.
   a. Define what an algorithm is.
   b. Describe the three characteristics of algorithms.
   c.
      i. Write an non-recursive algorithm in pseudocode, which receives two positive integers m and n, and returns the greatest common divisor of m and n, $gcd(m, n)$.
      ii. Draw the flowchart for your code above.

**************END OF TEST**************