FAST- National University of Computer and Emerging Sciences, Karachi.
FAST School of Computing, Fall 2024
CS1005-Discrete Structures
Assignment # 3

<u>Instructions:</u>   **Max. Points: 100**

1- This is hand written assignment.
2- Just write the question number instead of writing the whole question.
3- You can only use A4 size paper for solving the assignment.

---

1. What are the quotient and remainder when:
   a) 19 is divided by 7?   b) −111 is divided by 11?   c) 789 is divided by 23?
   d) 1001 is divided by 13?   e) 10 is divided by 19?   f) 3 is divided by 5?
   g) −1 is divided by 3?   h) 4 is divided by 1?

2. (a) Find a div m and a mod m when
   i) $a = -111$, $m = 99$.   ii) $a = -9999$, $m = 101$.
   iii) $a = 10299$, $m = 999$.   iv) $a = 123456$, $m = 1001$.

   (b) Decide whether each of these integers is congruent to 5 modulo 17.
   i) 80   ii) 103   iii) −29   iv) −122

3. (a) Determine whether the integers in each of these sets are pairwise relatively prime.
          i) 11, 15, 19   ii) 14, 15, 21   iii) 12, 17, 31, 37   iv) 7, 8, 9, 11

   (b) Find the prime factorization of each of these integers.

         i) 88   ii) 126   iii) 729   iv) 1001   v) 1111   vi) 909

4. Use the extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 100001) as a linear combination.

5. Solve each of these congruences using the modular inverses.
         a) $55x \equiv 34 \pmod{89}$ b) $89x \equiv 2 \pmod{232}$

6. (a) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences.
         i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.
         ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.

7. Find an inverse of *a modulo m* for each of these pairs of relatively prime integers.
         a) $a = 2$, $m = 17$ b) $a = 34$, $m = 89$
         c) $a = 144$, $m = 233$ d) $a = 200$, $m = 1001$

8. (a) Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
         i) $f(p) = (p + 4) \bmod 26$ ii) $f(p) = (p + 21) \bmod 26$

   (b) Decrypt these messages encrypted using the Shift cipher. $f(p) = (p + 10) \bmod 26$.
         i) CEBBOXNOB XYG   ii) LO WI PBSOXN

9. Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

   b) Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

10. (a) Encrypt the message I LOVE DISCRETE MATHEMATICS by translating the letters into numbers, applying the Caesar Cipher Encryption function and then translating the numbers back into letters.

(b) Decrypt these messages encrypted using the Caesar Cipher.
    i) PLG WZR DVVLJQPHQW   ii) IDVW QXFHV XQLYHUVLWB

<u>COUNTING TECH.:</u>

1. (a) Eight members of a school marching band are auditioning for 3 drum major positions. In how many ways can students be chosen to be drum majors?
   (b) You must take 6 CS elective courses to meet your graduation requirements at FAST-NUCES. There are 12 CS courses you are interested in. In how many ways can you select your elective Courses?
   (c) Nine people in our class want to be on a 5-person basketball team to represent the class. How many different teams can be chosen?

2. (a) A committee of five people is to be chosen from a group of 20 people. How many different ways can a chairperson, assistant chairperson, treasurer, community advisor, and record keeper be chosen?
   (b) A relay race has 4 runners who run different legs of the race. There are 16 students on your track team. In how many ways can your coach select students to compete in the race? Assume that the order in which the students run matters.
   (c) Your school yearbook has an editor in chief and an assistant editor in chief. The staff of the yearbook has 15 students. In how many ways can a student be chosen for these 2 positions?

3. (a) A deli offers 5 different types of meat, 3 types of breads, 4 types of cheeses and 6 condiments. How many different types of sandwiches can be made of 1 meat, 2 bread, 1 cheese, and 3 condiment?
   (b) Police use photographs of various facial features to help eyewitnesses identify suspects. One basic identification kit contains 15 hairlines, 48 eyes and eyebrows, 24 noses, 34 mouths, and 28 chins and 28 cheeks. Find the total number of different faces.

4. (a) How many bit strings of length 10 either begin with three 0s or end with two 0s?
   (b) How many bit strings of length 5 either begin with 0 or end with two 1s?

5(a) Show that if seven numbers from to 1 to 12 are chosen, then two of them will add upto 13.
  (b) If eight people are chosen, in any way from a group show that, atleast two of them will have been born on the same day of the week.
  (c) Show that if any 30 people are selected, then we may chose a subset of 5 so that all 5 were born