# FAST- National University of Computer and Emerging Sciences, Karachi.

## FAST School of Computing, Fall 2022

## CS1005-Discrete Structures

## Assignment # 3

**Instructions:** **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 $x \equiv 4 \pmod{11}$.

   (b) An old man goes to market and a camel step on his basket and crushes the oranges. The camel rider offers to pay for the damages and asks him how many oranges he had brought. He does not remember the exact number, but when he had taken them out five at a time, there were 3 oranges left. When he took them six at a time, there were also three oranges left, when he had taken them out seven at a time, there was only one orange was left and when he had taken them out eleven at a time, there was no orange left. What is the number of oranges he could have had?

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 $5^{2003} \bmod 13$.

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

11. (a) Which memory locations are assigned by the hashing function $h(k) = k \bmod 97$ to the records of insurance company customers with these Social Security numbers?
    i) 034567981 ii) 183211232 iii) 220195744 iv) 987255335

    (b) Which memory locations are assigned by the hashing function $h(k) = k \bmod 101$ to the records of insurance company customers with these Social Security numbers?
    i) 104578690 ii) 432222187 iii) 372201919 iv) 501338753

12. What sequence of pseudorandom numbers is generated using the linear congruential generator? $x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$? Do at least 20 iterations.

13. (a) Determine the check digit for the UPCs that have these initial 11 digits.
    i) 73232184434 ii) 63623991346

    (b) Determine whether each of the strings of 12 digits is a valid UPC code.
    i) 036000291452 ii) 012345678903

14. (a) The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881. What is the check digit for that book?

(b) The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.

15. 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.

16. (a) An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?
    (b) A particular brand of shirt comes in 12 colors, has a male version and a female version, and comes in three sizes for each sex. How many different types of this shirt are made?

17. (a) How many different three-letter initials can people have?
    (b) How many different three-letter initials with none of the letters repeated can people have?

**18.** **(a) A wired equivalent privacy (WEP) key for a wireless fidelity (WiFi) network is a string of either 10, 26, or 58 hexadecimal digits. How many different WEP keys are there?**
**(b) How many strings are there of four lowercase letters that have the letter x in them?**

**19.** **(a) How many functions are there from the set {1, 2, . . . , *m*}, where *m* is a positive integer, to the set {0, 1}?**
**(b) How many one-to-one functions are there from a set with five elements to sets with five elements?**

**20.** **(a) Use a tree diagram to determine the number of subsets of {3, 7, 9, 11, 24} with the property that the sum of the elements in the subset is less than 28.**

**(b) Teams A and B play in a tournament. The team that wins first two games wins the tournament. Use a tree diagram to find the number of possible ways in which the tournament can occur.**

**21.** **(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?**

**22.** **(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?**

**23.** **(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.**

**24.** **(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?**

**25.** **(a) Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.**
**(b) Assuming that no one has more than 1,000,000 hairs on the head of any person and that the population of New York City was 8,008,278 in 2010, show there had to be at least nine people in New York City in 2010 with the same number of hairs on their heads.**
**(c) There are 38 different time periods during which classes at a university can be scheduled. If there are 677 different classes, how many different rooms will be needed?**

**26.** **(a)What is the coefficient of $x^5$ in $(1 + x)^{11}$?**
**(b)What is the coefficient of $a^7b^{17}$ in $(2a – b)^{24}$?**

27. A class has 20 women and 16 men. In how many ways can you:
    (a) put all the students in a row?
    (b) put 7 of the students in a row?
    (c) put all the students in a row if all the women are on the left and all the men are on the right?

28. (a) Prove the statement: There is an integer $n > 5$ such that $2^n - 1$ is prime.
    (b) Prove that for any integer a and any prime number p, if p | a, P | (a + 1).

29. (a) Prove the statement: There are real numbers a and b such that $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$.
    (b) Prove that if $|x| > 1$ then $x > 1$ or $x < -1$ for all $x \in R$.

30. (a) Find a counter example to the proposition: For every prime number n, n + 2 is prime.
    (b) Show that the set of prime numbers is infinite.

31. (a) Prove by contradiction method, the statement: If n and m are odd integers, then n + m is an even integer.
    (b) Prove the statement by contraposition: For all integers m and n, if m + n is even then m and n are both even or m and n are both odd.

32. (a) Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.
    (b) Prove by contradiction that $\sqrt{2} + \sqrt{3}$ is irrational.

33. By mathematical induction, prove that following is true for all positive integral values of n.

    (a) $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = (n(n+1)(2n+1))/6$
    (b) $1+2+2^2 + \ldots + 2^n = 2^{n+1} - 1$ for all integers $n \geq 0$
    (c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{1}{4} n^2(n+1)^2$

34. As we have discussed, the practical application of all the topics in the class. Now you are required to submit at least two real world applications of the following topics.

    (a) Combination
    (b) Permutations
    (c) Binomial Theorem
    (d) Proof methods
    (e) Mathematical Induction

BEST OF LUCK ☺