Math 189 Fall 2021 Test III

Dr Holmes

December 13, 2021

This exam will be given in the final examination period, Monday Dec 13 12-2 pm. Two problems on the takehome are also part of this exam; they are due with the rest of the takehome at 11:55 pm Thursday Dec 16.

You are allowed the usual single sheet of notebook paper. You are also allowed to bring the takehome exam in and work on it during the final exam period if you have time.

You may use a calculator.

1. Induction proofs. Do both of these: the one you do better on counts 70 percent of the value of the question, and the other 30 percent.

   (a) Prove by induction that the sum $\Sigma_{i=1}^{n}(2i-1)$ of the first n odd numbers is equal to n^2.

(b) Prove by induction that n^3-4n+6 is divisible by 3 for any positive integer n.

The fact that $(n+1)^3 = n^3 + 3n^2 + 3n + 1$ will be useful.

2. Recursive definitions. We define $a_1 = 1; a_2 = 4; a_{n+2} = 5a_{n+1} - 6a_n$. Compute a_6 (of course you need to compute all terms of the sequence before it).

3. Display the addition and multiplication tables for mod 7 arithmetic. Then make tables (using the addition and multiplication tables you have constructed) of additive inverses of the numbers from 0 to 6 and multiplicative inverses of the numbers from 1 to 6 in mod 7 arithmetic.

4. Determine, using the extended Euclidean algorithm (showing all calculations) integers x and y such that $137x + 25y = \texttt{gcd}(137, 25)$.

   Your work should make it clear that you know what $\texttt{gcd}(137, 25)$ is, what x is, and what y is.

   What is the multiplicative inverse of 25 in mod 137 arithmetic?

5. Compute $23^{128} \bmod 100$. Hint: the exponent is a power of 2, and computing remainders mod 100 is dead easy.

6. My RSA key has modulus $N = pq = (23)(29) = 667$. My encryption exponent is 493. Someone sends you the message 631. Decipher it.

   Hint: you need to find the decryption exponent. I guarantee that it is much smaller than 493.

7. There is a committee of 12 members, 7 men and 5 women, which wants to develop some additional structure. The parts of this problem explore various aspects. Please give answers both in forms involving multiplication, division, permutations and/or binomical coefficients in a way which indicates that you understand the problem, and as final numerical answers.

   (a) In how many ways can the committee choose a president, secretary, and treasurer (these three officers will be three different members of the committee)?

(b) In how many ways can the committee choose a subcommittee with six members?

In how many ways can the commitee choose the subcommittee with six members with the extra requirement that it have the same numbers of men and women?

(c) In how many ways can the committee divide itself into working groups 1, 2, and 3, each with four members?

In how many ways can the committee divide itself into three subcommittees with four members? This is not quite the same question!

8. Do both of the two parts. The one you do better on will count for 70 percent of the value of the problem, and the other 30 percent.

   (a) In how many ways can you rearrange the letters in the word SUCCESS? Please write this both in terms of factorials to demonstrate that you know the method of solution and as a numerical answer.

(b) My wife has five politically correct bagel flavors (not including my favorite cranberry orange, sadness) and sends me to buy a baker's dozen (13) bagels selected from these flavors. In how many ways can this order be filled? Please write the answer both as a binomial coefficient (indicating knowledge of the procedure) and as a numerical answer.