Asn. 4 CMPUT 272 posted Nov 2 due before 1230 Nov 15
in CMPUT 272 box opposite room CSC 145 **show all work**

1. Write a statement acknowledging **all** resources consulted (discussions*, texts, urls, etc.) on this assignment. **Without this acknowledgement, your assignment will not be graded.** *Non-detailed oral discussion with others (inc. non-students) is permitted as long as any such discussion is summarized and acknowledged by all parties; the viewing or exchanging of any written work, even in rough or preliminary form, is expressly forbidden, as is any detailed discussion.

2. Alice and Bob create a DHM secret key with prime $p = 163$ and base $b = 72$, and respectively choose 19 and 111 as secret numbers s and t. (i) What number does Alice send Bob? (ii) What number does Bob send Alice? (iii) What is the secret key k they create? (iv) Explain how Eve (an eavesdropper) can discover k in this example.

3. Alice uses RSA with primes $p = 101$ and $q = 17$ and exponent $e = 99$. (i) Why is this choice of e ok? Find the inverse d. (ii) Why can Bob not send secret message $m' = 51$ to Alice? (iii) To send secret message $m = 1599$ to Alice, what encrypted number c does Bob send? (iv) How does Alice recover m from c?

4. Using a Venn diagram argument, for finite sets A, B, C prove or disprove (i) $(A - B) \cup (B - C) \subseteq A - C$ (ii) $A - C \subseteq (A - B) \cup (B - C)$.

5. Let $S = \{1, 2, \ldots, 9\}$. For each of the following, (i) in lexicographic order, list the first five and last five items (ii) give the total number of items, justifying briefly.

   (a) 4-sequences of S (b) 4-permutations of S (c) 4-subsets of S (d) 4-multisets of S.

6. (i) In lexicographic order, list the first five and last five 4-multisets of $\{1, 2, 3, 4, 5, 6\}$.

   For each of the ten multisets in (i), give (ii) the associated "$\bullet\,|$" diagram together with the 4-subset of $\{1, 2, \ldots, 9\}$ indicating the positions of the dots.

7. For $n \geq 0$, suppose that a fruit basket contains 1 orange, 1 apple, and $n - 2$ distinguishable bananas. Assume $k \geq 0$ is fixed. How many k-subsets of the set of n pieces of fruit contain (i) the orange? (ii) the apple? (iii) neither the apple nor the orange? (iv) What combinatorial identity have you just proved?

8. (i) For each $n = 15, 16, \ldots, 20$, list the units of n, namely the numbers in $\{1, \ldots, n-1\}$ that are relatively prime to n. (ii) For p prime, determine $\Phi(p^2)$, namely the number of units of p^2, and prove that your answer is correct.

9. Let $A(n)$ be this predicate: $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

   (i) Prove $A(0)$, $A(1)$, $A(2)$, and $A(3)$ by giving all the terms of the summation.

   (ii) Prove by induction that $A(n)$ holds for all nonnegative integers. In your proof, use this identity: for integers n and k with $n > k > 0$, $\displaystyle\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.