Homework 8

Due: Wednesday, April 10, 2024

All homeworks are due at 11:59 PM on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit.

Problem 1

Consider the following equation, where each x_i must be a non-negative integer:

$$x_1 + x_2 + x_3 + x_4 = 220$$

a. Count the number of solutions to this equation.

b. Now suppose we require a solution with x_1 and x_3 strictly positive. Count the number of solutions under this new constraint.

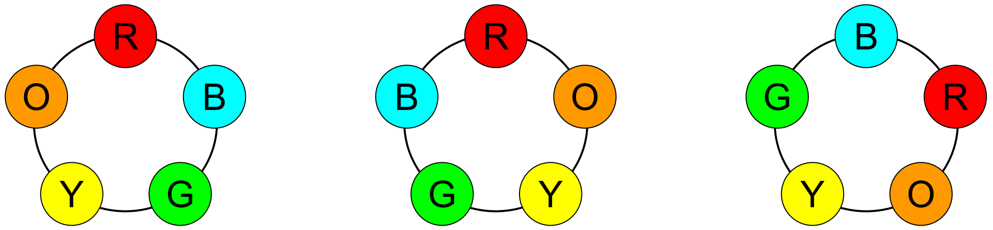
c. More generally, suppose we require a solution where a_1, a_2, a_3, and a_4 are fixed constant nonnegative integers and for each $1 \le i \le 4$, $x_i \ge a_i$, satisfying

$$\sum_{i=1}^{4} a_i \le 220.$$

Again, count the number of solutions under this new constraint. Your answer will be *symbolic*, that is, it will contain the expressions $a_1, \ldots, a_4$.

Problem 2

Pierre is a very fashionable dinosaur! He has 7 distinct bones: a red bone, an orange bone, a yellow bone, a blue bone, a green bone, a purple bone, and a pink bone. He designs necklaces by attaching 5 of his bones to a circular string. Two necklaces are identical if they have the same 5 colors and the same relative arrangement of colors around the circle. For example, these three necklaces are identical:



a. If Pierre designs one necklace per day for a year, prove that he will repeat at least one necklace design.

b. Pierre's friend gifts him a a pink bone that is identical to the pink bone that he already owns. Pierre now has 8 bones, two of which are indistinguishable. How many distinct 5-bone necklaces can Pierre design with this new set of bones?

Problem 3

We introduced the *binomial theorem* as an equation for expanding $(x+y)^n$. In this equation, the *binomial coefficients* $\binom{n}{k}$ represent the coefficients of the monomials $x^{n-k}y^k$.

Traditionally, though, $\binom{n}{k}$ represents the number of k-element subsets of a set with cardinality n. Here we establish a connection between these two ideas.

Prove, using the binomial theorem, that for any set of size $n > 0$, the number of its even-cardinality subsets is equal to the number of its odd-cardinality subsets. While there are many ways to prove this statement, such as creating a bijection or using induction, for this problem **you must use a counting argument with the binomial theorem.**

Hint: You will want to use a particular instance of the binomial theorem for this problem: that is, you will apply it to two particular values x and y. One way to start is to experiment with different inputs until you find some that seem helpful; another way is to work backward from the statement of the binomial theorem.

Problem 4 (Mind Bender — *Extra Credit*)

Bob encrypts a very secret message m and sends it to Alice, whose public key is (N, e), using RSA. Eve intercepts a copy of Bob's ciphertext c but, since it is encrypted, cannot obtain m.

Eve then sends Alice a ciphertext c' and asks Alice to compute and send back the corresponding decrypted message m'. Both Eve's ciphertext and message appear random to Alice (who has already received and decrypted Bob's original message), so Alice agrees to send m' to Eve. But once Eve receives m', she is able to obtain Bob's original secret message m!

a. Devise a strategy that Eve can use to pull this off, making sure to clearly describe how Eve computes c' and how she computes m once she has received m'. Explain why your proposed strategy avoids arousing Alice's suspicions, and prove that your strategy allows Eve to recover Bob's message. You should explicitly identify any nontrivial algorithms Eve needs to use in order to carry out her strategy.

   Note: your proposed strategy must be computationally feasible for large values of N. For example, your solution must not depend upon using brute force to factor N or to compute $\phi(N)$.

b. Suppose you are Eve. You know that Alice's public key is $(N, e) = (91, 5)$, and you intercept the ciphertext $c = 35$ from Bob. Using your strategy above, determine what Bob's secret message was!

   To obtain m' from Alice, enter your value c' into this page.

   Note: your response *must* use your algorithm from part (a) and must *not* involve factoring 91 or computing $\phi(91)$. You should show all steps of your algorithm, though you may use a calculator for multiplication and exponentiation mod N.