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 $1 \leq i \leq 4$, $x_i \geq a_i$, satisfying

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

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

Solution:

a. This is a straightforward example of "stars and bars." We need three "separators" to split 220 "units" between x_1, x_2, x_3, and x_4. So we lay out 223 spots and choose three of them to hold separators. That gives $\binom{223}{3} = 1,823,471$ solutions.

b. Let $u_1 = x_1 - 1$ and $u_3 = x_3 - 1$. Then the original equation (after substituting in for $x_1 = u_1 + 1$ and $x_3 = u_3 + 1$) becomes $u_1 + x_2 + u_3 + x_4 = 221$, where each of the terms on the left is a nonnegative integer.
This is the same problem as part (a), which we know how to solve.

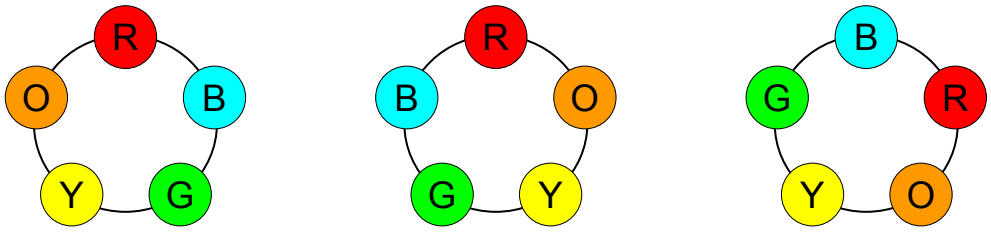
This clean representation allows us to use the same approach as in part (a), and the number of solutions is simply $\binom{221}{3} = 1,774,630$.

c. This is a similar problem to part (b), but we don't know what the a_i are.

Still, we can follow similar steps.
Define $u_i = x_i - a_i$ for i=1,2,3 and 4. Then our new equation after substitution is $u_1 + u_2 + u_3 + u_4 = 220 - \sum_{i=1}^{4} a_i$. Again each of the terms on the left is a nonnegative integer, so we can apply our function f from part (a). There are exactly $f(220 - \sum_{i=1}^{4} a_i) = \binom{223 - \sum_{i=1}^{4} a_i}{3}$ solutions to this equation. Thus the answer is $\binom{223 - \sum_{i=1}^{4} a_i}{3}$.

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?

Solution:

PART A:
Define N as the set of all distinct 5-bone necklaces that Pierre can make. Define D as the set of all days in the year. My proof plan is to find $|N|$, show that $|N| < |D|$, and then apply the pigeonhole principle.

1a. Calculating $|N|$ using Division rule

Define S as the set of all sequences of 5 distinct bones. We form such a sequence by selecting a 5-element subset of the 7 possible bones, then taking a permutation of that subset. Since there are $\binom{7}{5}$ 5-element subsets of the set of bones and 5! permutations of a 5-element set (regardless of which subset it is), it follows by the (dependent) multiplication principle that $|S| = \binom{7}{5} \cdot 5! = \frac{7!}{2!} = 2520$.

Define the function $f : S \to N$, where $f(s \in S)$ is the necklace $n \in N$ that would be formed if Pierre added each bone in s to his necklace in a clockwise manner.

f is 10-to-1. Since we can rotate necklaces, the permutations $(b_1, b_2, b_3, b_4, b_5)$, $(b_2, b_3, b_4, b_5, b_1)$, ..., $(b_5, b_1, b_2, b_3, b_4)$ are all indistinguishable (for fixed $b_1, \ldots, b_5$). Furthermore, since we can reflect a necklace without affecting pairwise adjacency,

these are all also indistinguishable from $(b_5, b_4, b_3, b_2, b_1)$, ..., $(b_4, b_3, b_2, b_1, b_5)$. In total, we have found that for any permutation $(b_1, b_2, b_3, b_4, b_5)$, there are 10 permutations that correspond to an equivalent necklace. Moreover, there are no other ways to form a new permutation that preserves pairwise adjacency. So each of these sets of 10 permutations in the S corresponds to one necklace in N, so we conclude that f is 10-to-1.

Since f is 10-to-1, we can use the division rule to show that $|S| = 10|N|$. It follows that $|N| = 252$.

2. Applying the pigeonhole principle

Define the function $f : D \to N$, where $f(d \in D)$ is the necklace that Pierre designed on day d. Since $|D| \geq 365 > 252 = |N|$, we know that $|D| > |N|$. Using the pigeonhole principle, it follows that there exists two days that Pierre designed the same necklace.

PART B:

(Note: this is a somewhat rough sketch of a solution, not a fully rigorous justification!)

Pierre can still make the 252 different necklaces he could make before. So it remains to count the new necklaces he can now make that he couldn't before, which are those that contain two pink bones.

To create such a necklace, he must pick the two pink beads (there's only one way to do this) as well as three of the six non-pink beads (there are $\binom{6}{3}$ ways to do this). Then he must arrange these five (two pink, three non-pink) beads in a circle. There are two methods to count how many ways he can do this.

One approach is to observe that, if we assume all beads are distinguishable, there are $\frac{5!}{10}$ ways to arrange them in a circle, as we showed in part (a). However, this overcounts by a factor of 2 because two of the beads are indistinguishable, so any permutations that swap their positions are actually the same necklace. So we need to divide by another factor of 2, yielding $\frac{5!}{20}$ circular arrangements.

Another way to think about this is that there are $\binom{5}{3} \cdot 3!$ ways to order the beads in *distinguishable* linear arrangements, then divide by 10 as before (using the same logic as part a for converting between linear permutations and circular ones). We justify the foregoing expression by noting that we can form distinguishable linear rearrangements of the beads by first selecting the two positions where are indistinguishable pink beads will go (there are $\binom{5}{3}$ ways to choose these), then ordering the 3 remaining (all mutually distinguishable) beads among the 3 remaining spots, which we can do in 3! ways. By the multiplication principle, there are then $\binom{5}{3} \cdot 3!$ ways to distinguishably linearly arrange the bones, as claimed. Thus, the total number

of circular arrangements is $\frac{\binom{5}{3}\cdot 3!}{10}$, which a straightforward computation shows to be equal to the expression we obtained above.

Finally, by the multiplication principle, there are

$$\binom{6}{3} \cdot \frac{5!}{20} = \binom{6}{3} \cdot \frac{\binom{5}{3} \cdot 3!}{10} = 120$$

ways to form a necklace with two pink beads. Adding this to our existing 252 ways to construct a necklace with 0 or 1 pink beads yields a total of 372 possible necklaces.

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.

Solution:

Proof. We can apply the binomial theorem to sum of 1 and -1:

$$\begin{aligned}(1-1)^n &= \sum_{k=0}^{n}(1)^{n-k}(-1)^k\binom{n}{k} \\ &= \sum_{k=0}^{n}(-1)^k\binom{n}{k}\end{aligned}$$

Since $(1-1)^n = 0^n = 0$, we have shown that

$$0 = \sum_{k=0}^{n}(-1)^k\binom{n}{k}$$

We can then separate the sum we have constructed into odd and even k values:

$$0 = \sum_{k \text{ odd}}(-1)^k\binom{n}{k} + \sum_{k \text{ even}}(-1)^k\binom{n}{k}$$

Since we know $(-1)^k = -1$ when k is odd, and $(-1)^k = 1$ when k is even, we have

$$0 = -\sum_{k \text{ odd}}\binom{n}{k} + \sum_{k \text{ even}}\binom{n}{k}$$

$$\sum_{k \text{ odd}} \binom{n}{k} = \sum_{k \text{ even}} \binom{n}{k}$$

We know that the term $\binom{n}{k}$ counts the number of size k subsets of a set of size n (since it counts the number of ways k items can be chosen out of n total items). Therefore, the left hand side of this equation counts the number of odd-sized subsets (subsets with odd cardinality), and the right hand side counts the number of even-sized subsets (subsets with even cardinality).

Hence we have shown that for any set of size $n > 0$, the number of odd-cardinality subsets is equal to the number of even-cardinality subsets. □

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.

Solution:

a. Eve picks some $k \in \mathbb{Z}$ such that $1 < k < N$.

   Since N has only two prime factors, it is exceedingly likely that k is invertible modulo N. In this case, Eve can compute her crafted ciphertext $c' \equiv k^e c \pmod{N}$ (computing powers mod N can be done efficiently). Alice will send back the "decrypted" value $m' \equiv (k^e c)^d \equiv (k^e m^e)^d \equiv km \pmod{N}$. Since we know k is invertible mod N, Eve can easily compute k^{-1} mod N using the extended Euclidean algorithm and then compute $k^{-1}m' \equiv k^{-1}km \equiv m \pmod{N}$, recovering Bob's message.

If k is not invertible modulo N, Eve could just pick a new k—since N has only two factors, she has high probability of picking some k relatively prime to N. However, Eve can use a much simpler approach if k is not invertible modulo N. In this case, we know that $\gcd(k, N) > 1$ by the linear combination theorem. But since $N = pq$ and $k < N$, we must have that $\gcd(k, N) = p$ or $\gcd(k, N) = q$. Without loss of generality, let's say $\gcd(k, N) = p$. In this case, Eve simply computes $\gcd(k, N) = p$ using the Euclidean algorithm, then finds $N/p = q$ and thus can find $\phi(N) = (p-1)(q-1)$. Then she uses the extended Euclidean algorithm to compute $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ and decrypts Bob's message by computing $c^d \equiv (m^e)^d \equiv m \pmod{N}$.

b. Let's pick $k = 2$, so $k^{-1} \equiv 46 \pmod{91}$. We compute $k^e = 2^5 \equiv 32 \pmod{91}$, so $c' \equiv k^e c \equiv 32 \cdot 35 \equiv 28 \pmod{91}$. Alice tells us that $m' = 84$, whence we have that $m \equiv k^{-1} m' \equiv 46 \cdot 84 \equiv 42 \pmod{91}$. So $m = 42$.