Homework 8

Due: Friday, April 11, 2025

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.

Problems marked with a * are problems which may appear on the midterm or final with some modification.

Problem 1

Recall from class that sets A and B have equal cardinality (i.e. $|A| = |B|$) if there exists a function $f : A \to B$ that is bijective. This allows us to compare the cardinality of two sets, even when the sets have infinite cardinality. For example, in class we saw that there exists a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ which shows $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ (you may assume this for this problem).

Show that all of the following sets have cardinality equal to the cardinality of the integers $|\mathbb{Z}|$ by giving a function that is a bijection from the set to $\mathbb{Z}$; you don't need to prove that your function is bijective, just give the function.

a. The even integers $\mathbb{Z}_{\text{even}}$.*
b. The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.*
c. All triples of natural numbers $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

Solution:

a. Define as our bijection $f(n) = \frac{n}{2}$.
b. Define as our bijection

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n+1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

c. Let g be the bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ that we saw in class and let h be the bijection from $\mathbb{N}$ to $\mathbb{Z}$ from the previous part. Then, given a triple of natural

numbers (a, b, c) for $a, b, c \in \mathbb{N}$, we let our bijection be

$$f((a, b, c)) = h(g(g(a, b), c)).$$

Problem 2

Rob is choosing a new exciting password. The requirements for his (case-sensitive) password are that:

- The password must consist of 5 or 6 valid characters.
- A valid character is either a lower case letter ("a" through "z" of which there are 26), an upper case letter ("A" through "Z" of which there are 26) or the symbol "!".
- The password must include exactly one "!".

For example, some valid and distinct passwords are "CSYa!", "CsYa!" and "Cs!Yay".

a. Give the number of possible passwords. Justify your answer using (formal or informal) counting rules.*

b. Suppose we add the additional constraint to the passwords that

   - The first letter can be upper or lower case (even if it occurs after the "!") but each letter must be the opposite case of the previous letter. Here, if a letter occurs just after "!" but is not the first letter, then it must be the opposite case of the letter just before the "!"

   For example, with this additional constraint, some valid and distinct passwords are "CsYa!", "cSyA!", "Cs!YaY", "cS!yAy", "!cSyAy" and "!CsYaY".

   Give the number of possible passwords with this additional constraint. Justify your answer using (formal or informal) counting rules.*

Solution:

a. We can break the task of choosing an n-character passwords for $n \in \{5, 6\}$ into choosing the position for our required "!" and then, for each of our remaining $n - 1$ characters, choosing a lower or upper case letter. The number of choices for our "!" is n. By the sum rule, the number of choices of lower or upper case letters is $26 + 26 = 52$.

   Thus, by the product rule, the number of n-character passwords for $n \in \{5, 6\}$ is therefore

$$n \cdot 52^{n-1}.$$

   Lastly, by the sum rule the number of possible passwords is equal to the number

of 5-character passwords plus the number of 6-character passwords and so the total number of passwords is

$$6 \cdot 52^5 + 5 \cdot 52^4 = 2317782272.$$

b. We can break the task of our choosing an n-character passwords for $n \in \{5, 6\}$ into choosing the position for our required "!", choosing the case for the first letter and then choosing each letter (without regards to their case). Again, the number of choices for our "!" is n. There are 2 possible choices for the case of the first letter. Once we choose the case of the first letter, this fixes the case of every letter and so there are only 26 possible choices for every letter (including the first letter).

Thus, by the product rule, the number of n-character passwords for $n \in \{5, 6\}$ is therefore

$$n \cdot 2 \cdot 26^{n-1}.$$

Lastly, by the sum rule the number of possible passwords is equal to the number of 5-character passwords plus the number of 6-character passwords and so the total number of passwords is

$$6 \cdot 2 \cdot 26^5 + 5 \cdot 2 \cdot 26^4 = 147146272.$$

Problem 3

Consider the following equation with variables $\{x_1, x_2, x_3\}$:

$$x_1 + x_2 + x_3 = 200$$

In each of the following parts, be sure to justify your answer.

a. Count the number of solutions to this equation which satisfy $x_i \geq 0$ and $x_i \in \mathbb{Z}$ for every i. Some example distinct solutions are: $x_1 = 0$, $x_2 = 190$, $x_3 = 10$, and $x_1 = 198$, $x_2 = 1$, $x_3 = 1$.*

b. Now, suppose we additionally require that our solution has $x_1 > 0$. Count the number of solutions with this additional constraint.

c. Finally, we require (in addition to the restriction in part b.) that $x_2 = x_3$. Count the number of solutions with this additional constraint.

Solution:

a. This is an example of "stars and bars." In particular, we need two "bars" to split 200 "stars" between x_1, x_2, and x_3. The formula for stars and bars says that the number of such placements is

$$\binom{202}{2} = 20301.$$

b. Let $u_1 = x_1 - 1$. Notice that $x_1 > 0$ iff $u_1 \geq 0$. Thus, we may substitute $x_1 = u_1 + 1$ to get that our goal is a solution to

$$u_1 + 1 + x_2 + x_3 = 200$$

where $u_1, x_2, x_3 \geq 0$ which is equivalent to

$$u_1 + x_2 + x_3 = 199$$

where $u_1, x_2, x_3 \geq 0$.

As in the previous part, this is a stars and bars counting problem with 2 bars and 199 stars and so there are

$$\binom{201}{2} = 20100.$$

c. The number of solutions to this is the same as the number of solutions to $x_1 + x_2' = 200$ with $x_1 > 0$ and x_2' even, which is the same as the number of solutions to $x_1' + x_2' = 199$ with x_2' even.

Ignoring the evenness constraint, there are $\binom{200}{1} = 200$ solutions to this. We claim that in exactly half of these solutions x_2' is even. We prove this claim by showing a bijection between solutions with x_2' even and solutions with x_2' odd.

Suppose (x_1', x_2') is a solution with x_2' even. Since $x_1' + x_2' = 199$, we have $x_1' \geq 1$, since it must be odd. This means that $(x_1' - 1, x_2' + 1)$ is a solution with x_2' odd.

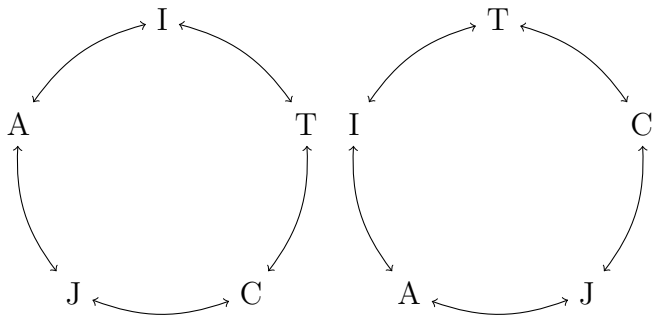
In reverse, if (x_1', x_2') is a solution with x_2' odd, then $(x_1' + 1, x_2' - 1)$ is a solution with x_2' even. This map is a bijection.

Thus we conclude that there are 100 solutions.

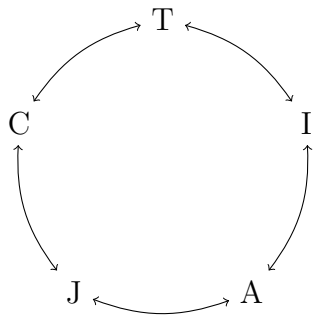
Problem 4

The 5 CS22 HTAs are in a circular standoff. Two standoffs are the same if they involve the same participants in the same order going clockwise.

For instance, these standoffs are the same:



This one is different from the two above:



a. Unbeknownst to the other HTAs, Amy and Christina have secretly made a pact and must always stand next to each other. In how many ways can the HTAs form their standoff? Justify your answer.

b. Rob and Ellis hear about the standoff and want to join, but there is only enough room for 5 people in the standoff. In how many ways can the HTAs with Rob and Ellis form their standoff? (Assume Amy and Christina can stand anywhere. As much as Rob and Ellis want to participate, we will count arrangements that exclude either or both of them.) Justify your answer.

c. Suppose Amy and Christina must stand next to each other, but only if they are both in the 5 people chosen to be in the standoff. (For example, if Christina is in the standoff and Amy is not, then there are no restrictions on where Christina can stand.) In how many ways can the HTAs with Rob and Ellis form their standoff with this added restriction? Justify your answer.

Solution:

a. If Amy and Christina must always stand next to each other, then we can treat them as a unit. Then, this is a circular seating problem with 4 people, so there are $(4-1)! = 3!$ ways to form a standoff with Amy and Christina as 1 unit. Since there are 2 ways to permute Amy and Christina (Amy can stand to the left of Christina or to the right, creating 2 different permutations), there are $2 \cdot 6 = 12$ possible permutations the HTAs can form in their standoff.

b. There are $\binom{7}{5} = 21$ ways to pick the 5 people in the standoff and $(5-1)! = 4! = 24$ ways to permute them in the standoff. Therefore, the total number of possible standoffs is $21 \cdot 24 = 504$.

c. We can solve for this by dividing the problem into 4 cases. Case 1: Amy and Christina are both in the standoff Then, there are $\binom{5}{3} = 10$ ways to choose the remaining 3 people to be in the standoff, and, from part a, we can conclude there are 12 ways to permute the 5 people in the standoff. Therefore, the total number of permutations is $10 \cdot 12 = 120$. Case 2: Amy and Christina are both not in the standoff Then, the remaining 5 people must be in the standoff, so there is only 1 way to choose the 5 people to be in the standoff. Since Amy and Christina are not both in the standoff, this becomes a standard circular seating problem, and there are $(5-1)! = 4! = 24$ ways to permute the 5 people in the standoff. Therefore, the total number of permutations is $1 \cdot 24 = 24$. Case 3: Amy is in the standoff but Christina is not Then, we must choose 4 other people to be in the standoff from the remaining 5 HTAs that are not Christina, meaning there are $\binom{5}{4} = 5$ ways to choose the remaining 4 people to be in the standoff. Since Amy and Christina are not both in the standoff, this becomes a standard circular seating problem, and there are 24 ways to permute them. Therefore, the total number of permutations is $\binom{5}{4} \cdot 24 = 120$. Case 4: Christina is in the standoff but Amy is not This is the same as case 3, meaning the total number of permutations is 120. Since these 4 cases cover all possible cases, the total number of possible standoffs is $120 + 24 + 120 + 120 = 384$.

Problem 5

Suppose that n is a natural number, and consider the following identity:

$$\binom{2n}{2} = 2\binom{n}{2} + n^2$$

a. For which values of n does this identity hold? It may be true for all natural numbers, for all n above some lower bound, or for all n below some upper bound. Come up with a hypothesis for this question in advance. You may want to come back and change your hypothesis after working on the following parts.

b. Prove that the identity holds for all n meeting your condition in part a. using a counting argument. That is: define a set X such that both sides of the identity describe the number of elements in this set.

c. Prove the same statement using an algebraic argument. That is: expand the definition of $\binom{n}{k}$ in terms of factorials, and compute.

Solution:

a. It holds for all $n \in \mathbb{N}$.

b. The left hand side of the identity counts the number of two-element subsets of a set with $2n$ elements.

Suppose that this set is partitioned into two subsets each of size n. $2\binom{n}{2}$ counts the number of ways to choose two elements from either partition (with both chosen elements coming from the same partition). To match the left hand side, we also need to count the subsets containing one element from each of the partitions. There are $n \cdot n = n^2$ of these.

c.

$$\begin{aligned}\binom{2n}{2} &= \frac{(2n)!}{2!(2n-2)!} \\ &= \frac{(2n)!}{2(2n-2)!} \\ &= \frac{2n(2n-1)}{2} \\ &= 2n^2 - n\end{aligned}$$

$$\begin{aligned} 2\binom{n}{2} + n^2 &= 2\frac{n!}{2!(n-2)!} + n^2 \\ &= 2\frac{n(n-1)}{2} + n^2 \\ &= n^2 + n(n-1) \\ &= 2n^2 - n \end{aligned}$$

Problem 6 (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 $m = 42$.