Encryption and Intro to Counting

Recitation 7

An Interactive Look at Encryption

Think back to the first time a teacher caught you passing a note in class: Wouldn't it have been cool if that note looked like complete nonsense to your teacher but made sense to you and your friend?

The purpose of encryption is to allow people to communicate securely over some medium. Without secure cryptosystems (RSA, for example), we wouldn't be able to purchase goods on the web without the fear of someone stealing your credit card information.

Suppose that Tim and Peet want to send secret messages to each other. They decide to replace letters with their order in the alphabet (that is, $A = 1$, $B = 2$, etc.). Note that Z can be either 26 or 0.

They agree on the following *encryption* and *decryption* functions:

$$en(x) = \text{rem}(3x, 26)$$

$$de(m) = \text{rem}(9m, 26)$$

Task 1

a. Tim sends Peet their next meeting place with the encrypted message $(22, 10, 11, 8, 19)$. Where are they meeting? You can use a calculator such as Wolfram Alpha.

b. Now, you try encrypting a four-letter word of your choosing and then decrypt it to see if it's the same message.

c. Why does Tim and Peet's encryption scheme work for this 26 character alphabet, that is, why can any encrypted digit be recovered exactly by the decryption process?

   Hint: What is the relationship between 3, 9, and 26?

   Since there are 26 letters in the alphabet, we can map every letter to a unique value, allowing any encrypted digit be recovered exactly.

d. *Optional:* Would this scheme work if the modulus was 23? What about 29? Assume you can change the other constants in the encryption and decryption functions.

RSA Encryption

Tim and Peet realize that their encryption scheme, is nicely simple, but is altogether too insecure. They opt instead to use RSA encryption to send notes to each other in class. Recall that the RSA encryption algorithm works as follows:

1. Choose two primes p, q.
2. Calculate $n = pq$. We can publish n publicly while keeping p, q private because factorization is a hard problem.
3. Calculate $\phi(n) = (p-1)(q-1)$.
4. Choose some $1 < e < \phi(n)$ such that $\gcd(e, \phi(n)) = 1$.
5. Find a multiplicative inverse d for e such that $de \equiv 1 \pmod{\phi(n)}$. A multiplicative inverse has to exist because e is defined to be relatively prime to the modulus.
6. Publish n (the modulus) and e (the encryption exponent).
7. Keep all other numbers private to yourself, but remember d: It will be your decryption exponent.

To encrypt a message m, compute $m^* = \text{rem}(m^e, n)$. To decrypt an encrypted message m^*, calculate $\text{rem}((m^*)^d, n)$.

Task 2

a. Now, create your group's own personal RSA key by choosing **large** prime values of p and q with 10 digits—use an online list of primes as a reference. (We want a larger modulus so we can send longer messages, but not so long that calculators can't handle it.) Write p, q, n, and $\phi(n)$ down here:

b. Now, find a pair of multiplicative inverses e and d modulus $\phi(n)$. You can use any online calculators/generators (we recommend Wolfram Alpha) to help you with things like prime factorization or solving congruencies.

c. Now, "publish" your n and e by posting them on this EdStem post. Your TAs will send you an encrypted message via a follow-up to your comment, which you'll have to decrypt to get checked off at the end of this section.

Checkpoint 1 - Call a TA over!

Counting

The Product Rule

Given finite sets $S_1, S_2, ..., S_n$, the product rule tells us that

$$|S_1 \times S_2 \times ... \times S_n| = |S_1| \cdot |S_2| \cdot ... \cdot |S_n|.$$

This rule is often useful when we are doing counting and what we are counting comes from some number of independent choices. For instance, when picking an outfit for the day, say you have 4 shirts, 3 pants, and 2 pairs of shoes to choose from. We can think of an outfit as a sequence (shirt, pant, shoe), so to find the total number of outfits, we multiply the number of choices we can make for each position, $4 \cdot 3 \cdot 2 = 24$.

Even if our choices depend on each other, we can still sometimes use this concept. For instance, let's say that for each of our 4 shirts, one of our 3 pairs of pants looks terrible with it, so we don't want to wear those pants if we're wearing that shirt. Then, we still have 4 choices for our shirt, but having made that choice, we now only have 2 pants to choose from. We still have 2 shoe options. So, our total number of outfit choices is $4 \cdot 2 \cdot 2 = 16$.

Task 3

a. Suppose we go to the sandwich shop, and we want to order a combo special. The combo special includes a sandwich, and side, and a drink.

   There are 5 different kinds of sandwiches, 6 different kinds of sides, and 8 different kinds of drinks. How many different ways could we order a combo special, and why?

b. When we first talked about functions, these functions only took in one input. Since then, we've seen propositions, which are functions that can take in more than one input! In general, functions can take in one or more inputs.

   Note that, if the function takes in more than one input, say n inputs, we can *think of it* taking in one input, where each input is a tuple of length n.

   i. Consider a function of 3 inputs, where each input value can be 0, 1, 2, or 3. If we think about this function as a function of one input, how many possible inputs does it have?

   ii. Consider a function with the same input as described above. Its output for each input is either 0 or 1. How many *unique* functions are there?

   Hint: Two functions are identical if every input leads to the same output.

iii. Consider functions of 2 inputs, where each input can take on 0, 1, or 2, and the function must output to 0 or 1. How many such functions are there?

iv. *Optional:* Consider functions of 2 inputs, where each input can take on either 0 or 1 and outputs either 0 or 1, but the order of the inputs does not affect that output of the function. For example, $f(x, y)$ could be $(x \wedge y)$. How many possible such functions are there?

Permutations and Counting Subsets

A permutation of a set A is an ordered list of the elements of A.

Task 4: Explain why there are $n!$ different permutations of a set of size n.

Let $|A| = n$. Let's say we want a permutation of k elements of A, where $k \leq n$. We could make such a permutation by picking one of n elements for the first position, $n-1$ elements for the second, etc, getting us $n*(n-1)*...*(n-k+1)$ permutations. We can also write this quantity

$$\frac{n!}{(n-k)!}.$$

How could we have gotten that same result in a different way? Well, we could have made all $n!$ permutations of A, and then grouped those based on the ordering of the first k elements. Each ordering of k elements has $(n-k)!$ possibilities for the order of the elements that follow it, hence we divide by $(n-k)!$.

Suppose we want to know the number of subsets of size k of a set of size n. The general formula for this value, called $\binom{n}{k}$ is

$$\frac{n!}{(n-k)!k!}.$$

Why? First, we can think of the permutations of length k of elements of A, which there are $\frac{n!}{(n-k)!}$ of. Then, we can group these with the other permutations that have the same elements but in a different order, and divide our count by the number in each group. How big is each group? For any set of k elements, there are $k!$ ways to order them. So, we divide by $k!$.

Try it out with a small example set to make sure it makes sense to you—perhaps with the number of ways to pick 2 astronauts out of a crew of 9?

Task 5: Count the size of each set, and sort them from largest to smallest.

a. The number of permutations of all the letters in the alphabet.

b. The number of subsets of size 6 of the letters of the English alphabet (one such subset is $\{a, b, c, d, e, f\}$).

c. The number of 6 letter words made of non-repeating letters (one such 6-letter word is "abcdef").

d. The number of (any sized) subsets of the set of the letters in the English alphabet.

e. The number of subsets of size 20 of the letters of the alphabet.

Task 6: Consider a string of size $n \geq 2$, $S = s_1 s_2 ... s_n$, where each s_i is a 1–9 digit. For each of the following conditions, find the number N of such strings that satisfy the condition, and prove your answer.

a. Only x types of digits are used, where $1 \leq x \leq 9$.

b. No two *consecutive* digits are the same.

c. *Optional:* The sum of any k consecutive digits is the same, where $1 \leq k \leq n$.

d. *Optional:* The product of any set of k consecutive digits is the same, where $1 \leq k \leq n$.

Task 7: By now, you should've received an encrypted message from your TAs. Use your private decryption exponent d to decrypt and read the message. More information about how to interpret the plaintext message is on the Campuswire post.

Checkpoint 2 - Call over a TA!

Counting Arguments

A counting argument shows that the LHS (lefthand side) and the RHS (righthand side) of some equation count the same thing. Instead of using algebraic manipulation, we explain why both sides enumerate the elements of some set, just in different ways.

For instance, consider the following identity.

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Let S be a set with n elements.

- The LHS counts the number of ways to form a subset of S size k.
- The RHS also counts the number of subsets of size k. It partitions it into two parts:
  - k-sized subsets **with** a fixed element x. Since we already know x is in the subset, so we just want to pick $k-1$ more elements from the $n-1$ remaining elements.

– k-sized subsets **without** x. We know we can't pick x for our subsets, so we just choose k elements from $n-1$ other elements in S.

Task 8

Use counting arguments to prove the following identities:

a.
$$\binom{n}{k} = \binom{n}{n-k}$$

b.
$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

c. *Optional:*
$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

Hint: Try this with small numbers where $k < m < n$.

Task 9

Below is a table of counting problems involving putting k balls in n distinct bins, and seven expressions. Match each problem with its solution.

	No restrictions	At **most** 1 ball per bin assume $k \leq n$	At **least** 1 ball per bin assume $k \geq n$
Identical balls	①	③	⑤ *Optional*
Distinct balls	②	④	⑥ *Optional*

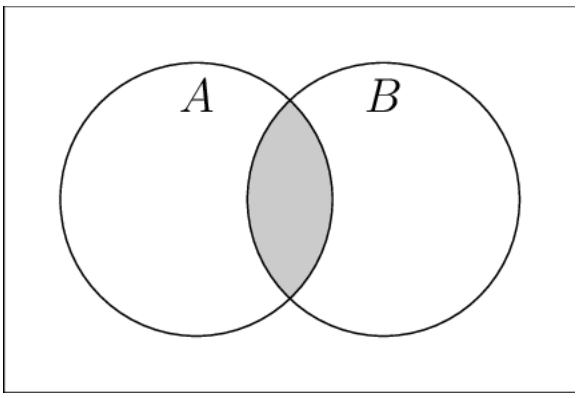
A	**B**	**C**	**D**	**E**	**F**	**G**
$\binom{n}{k}$	n^k	$\binom{k-1}{n-1}$	$\frac{n!}{(n-k)!}$	$\binom{k+n-1}{k}$	$n^k - \sum_{i=1}^{n-1}\binom{n}{i}(n-i)^k(-1)^{i+1}$	$n!\binom{k}{n}n^{k-n}$

Checkpoint 3 - Call over a TA

Inclusion/Exclusion

Say we have two sets, A and B, and we want to know how many elements there are in their union, $A \cup B$. If A and B have no elements in common, we can compute this just by adding the cardinality of each, $|A| + |B|$. However, this approach will not work in general.

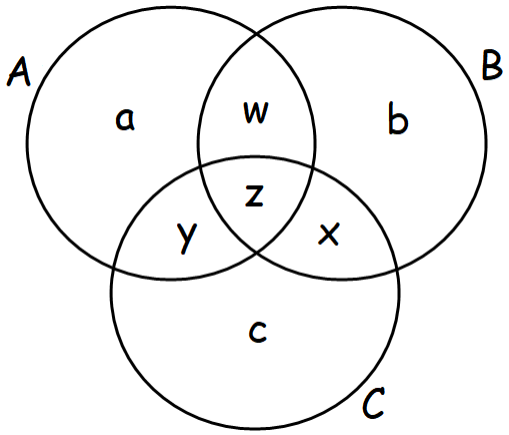
For instance, if $A = \{1, 2\}$ and $B = \{1, 3\}$, then $A \cup B = \{1, 2, 3\}$. $|A \cup B| = 3$, but $|A| + |B| = 2 + 2 = 4$. The problem is that we've double counted the elements that are in both A and B, that is, element 1. To fix this problem, we should subtract $|A \cap B|$.



The resulting Inclusion/Exclusion property for two sets is:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Let's try generalizing this idea to three sets, A, B, and C!



If we tried adding $|A| + |B| + |C|$, which regions would we double count? Which regions would we triple count?

As it turns out, the final formula for $|A \cup B \cup C|$ is the following. Convince yourself that it works!

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$

Going further, we can repeat this process for any number of sets, alternating between adding and subtracting the sizes of sets.

Task 10

d. Let $S = \{1, 2, 3, 4, 5\}$.

   i. How many permutations of S contain the sequence 24?

   ii. How many permutations of S contain the sequence 52?

e. Let X and Y be sets such that $|X| = 8$ and $Y = \{a, b, c\}$.

   i. How many functions from $X \to Y$ do not map to a?

   ii. How many functions from $X \to Y$ do not map to a and also do not map to b?

   iii. How many functions from $X \to Y$ are *not* surjective?

   Hint: A function is not surjective if nothing maps to a, nothing maps to b, or nothing maps to c.

The Pigeonhole Principle

Let's say we have n pigeons who are trying to fit in $n - 1$ holes.

It isn't possible for each pigeon to get its own hole: at least two of them are going to have to share. It could be the case that they are all in the same hole, or, like the picture above, all but 2 pigeons get their own hole, or anything in between.

This is the Pigeonhole Principle: in general, if we are assigning n objects to m categories, where $n > m$, there is at least one category that has more than one object assigned to it.

Solve the following problems using the Pigeonhole Principle:

Task 11

f. Celeste is pulling socks out of her drawer. She only has four types of socks: solid, striped, polka-dotted, and ones with planets on them. What is the minimum number of socks Celeste should pull out to ensure she has a pair?

g. There are $n > 2$ astronauts having a party on Mars. Throughout the night, they dance with each other in pairs.

   i. The minimum number of total dance partners someone can have is 0 (they didn't dance with anyone). What is the maximum number of dance partners one can have?

   ii. Prove that at least 2 astronauts have the same number of dance partners by the end of the night. (Come back to this question later if you get stuck.)

h. Suppose S is a set of $n + 1$ integers. Prove that there exist distinct $a, b \in S$ such that $a - b$ is a multiple of n.

i. *Optional:* Given any 5 points inside a square with side length 2, there is always a pair whose distance apart is at most square root of 2.

Checkoff - Call over a TA