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.

Solution:

PLUTO

rem(9*22, 26) = 16
rem(9*10, 26) = 12
rem(9*11, 26) = 21
rem(9*8, 26) = 20
rem(9*19, 26) = 15

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

Solution:

Almost any four-letter words the students pick is fine, as long as their work looks OK and they seem to understand the process.

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?

Solution:

First, we note that 3 has a multiplicative inverse mod 26 (specifically, 9). Therefore, rem(3x, 26) has a distinct answer for each x in [0, 25]. The map $x \to 3x \pmod{26}$ is a bijection with inverse $x \to 9x \pmod{26}$.

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.

Solution:

It would not work if the modulus was 23 because the range of the function would be reduced to $[0, 22]$. We'll lose some of the letters towards the end of the alphabet.

However, it *would* work with $m = 29$—in fact, we'll be able to support 3 extra characters to take on the values 27, 28, and 29.

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:

> **Solution:**
>
> TAs - make sure that p and q are large! The modulus has to be greater than any message we want to send, which we restricted on our end to be 18 digits or less.

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.

> **Solution:**
>
> TAs - just ask how they did this part to make sure they understand what's going on. One way of finding a e is just prime factorizing $\phi(n)$ and making a new number that doesn't share any of those numbers. Then, plug $de \equiv 1 \pmod{\phi(n)}$ into Wolfram Alpha to solve for d. In class, we pointed out that picking a random number in the right range and running Euclid will work quickly and accurately.

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?

> **Solution:**
>
> 240. We let A be the set of sandwiches, B be the set of sides, and C be the set of drinks. Then $A \times B \times C$ has all of the different ways we could order, and there are $5 \cdot 6 \cdot 8 = 240$ elements in this Cartesian product.

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?

Solution:
There are 4 options for each position in the input, so 4^3.

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.

Solution:
There are 4^3 inputs, as described above. There are 2 options for what each can map to, so $2^{(4^3)}$ functions.

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?

Solution:
Same logic as before, $2^{(3^2)}$.

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?

Solution:
This time, we consider the possible input sequences: $(0, 0), (0, 1), (1, 0), (1, 1)$. Because $f(0, 1) = f(1, 0)$, once we choose where one maps to, we have to choose the same thing for the other, so we effectively only have a choice for 3 inputs, or 2^3.

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.

Solution:

n options for the first position, $n-1$ for the second, etc. gives us $n \cdot (n-1) \cdot ... \cdot 1$.

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.

Solution:

1. $26!$
2. $\binom{26}{6} = \frac{26!}{20!*6!}$
3. $\frac{26!}{20!}$
4. 2^{26}
5. $\binom{26}{20} = \frac{26!}{20!*6!}$

1, 3, 4, 2 = 5

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 $1 \leq x \leq 9$.

Solution:

There are n digits, each of which has x options, meaning there are x^n possibilities.

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

Solution:

The first digit has 9 options. The remaining digits have 8 options since they cannot match the preceeding digits. Thus, there are $9 \cdot 8^{n-1}$.

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

Solution:

Consider some arbitrary sequence of k digits of the number $s_i s_{i+1} ... s_{i+k-1}$ with sum r. Now, if we move on to the next k digits with s_2 at the front, we seek

the sum of $s_{i+1}s_{i+2}...s_{i+k}$. We know that each k group must have the same sum, r, so

$$s_{i+1} + s_{i+2} + ... + s_{i+k} = r$$

But we know from the first k digits that

$$r - s_i + s_{i+k} = r$$

which implies that $s_{k+i} = s_i$. This means that, for all k-sequences to have the same sum, a particular k sequence must be cycled through in order. This implies that counting the number of k sequences possible is sufficient. Since there are k digits to choose, there are 9^k such options.

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

Solution:

The argument is the same as above. The only step that changes is

$$s_{i+k}r/s_i = r$$

which still implies that $s_{k+i} = s_i$. There are similarly 9^k options.

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.

Solution:

Our default message was 1309121125230125, "MILKYWAY". More creative TAs may have sent you a different message.

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.

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

Solution:

The LHS is the number of ways to choose k elements from a set of size n, which can be equivalently seen as the number of ways to choose $n-k$ elements *not* to include, which is what the RHS counts.

b.

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

Solution:

The LHS is the number of subsets of each size of a set of size n added together. In other words, we can count the number of subsets with 0 elements ($\binom{n}{0}$), the number of subsets with 1 element ($\binom{n}{1}$), and so on. If we add them up, we will get $\sum_{k=0}^{n} \binom{n}{k}$.

Alternatively, the RHS is the total number of subsets of a size of size n. This is because, for each element, we can choose to either contain it in the subset, or not contain it in the subset. Thus, for each of the n elements, we have 2 options: include or don't include. That gives us $2 \cdot 2 \cdot ... \cdot 2 = 2^n$ different subsets.

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

c. *Optional:*

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

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

Solution:

The LHS is the number of ways to choose m members of a general committee, and then choose k special members from that m for a subcommittee. The RHS is the number of ways to choose k members of a special subcommittee, and then the number of ways to include the unpicked members in the general committee of size m, but it only has $m - k$ spots left.

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	$\binom{k-1}{n-1}$	$\frac{n!}{(n-k)!}$	$\binom{k+n-1}{k}$	$n^k - \sum_{i=1}^{n-1} \binom{n}{i}(n-i)^k(-1)^{i+1}$	$n!\binom{k}{n}n^{k-n}$

Solution:

1. This is stars and bars, so it's E.

2. Each of the k balls have n options, so it's B.

3. We have n bins and k of them will have 1 ball in them. There is a bijection between this situation and n-bit binary strings with k ones and $n-k$ zeros. So, this is choosing which digits will have 1s, which is A.

4. For each of the options from question 3, which is $\binom{n}{k}$, there are $k!$ ways of scrambling the balls in sequence. So we have $\frac{n!}{k!(n-k)!}k!$, which cancels out to D. Note this is also the permutation $P(n,k)$.

5. This can be reduced to stars and bars, but we pre-distribute n balls to the n bins to make sure there's 1 in each bin. Then, with the $k-n$ balls left, we distribute it into k bins, which is $\binom{k-n+n-1}{n-1} = \binom{k-1}{n-1}$, which is C.

6. We'll count the ways there is a bin with *no* balls, using inclusion-exclusion, and find the complement of that. Let E_j be the event that the j-th bin is empty, and we want to find $|E_1 \cup \cdots \cup E_n|$. Each E_j is of size $(n-1)^k$, since the k balls can go to any of the $n-1$ other bins. Then we take out the pairwise intersections, each of which are of size $(n-2)^k$, and so on to $(n-i)^k$ generally. The number of i-way intersections is $\binom{n}{i}$, which we also have to multiply by. To include all of this in a summation, along with using $(-1)^{i+1}$ to simulate the alternating addition/subtraction. Note that the last term, $i = n$, is always zero (why?). This is expression F.

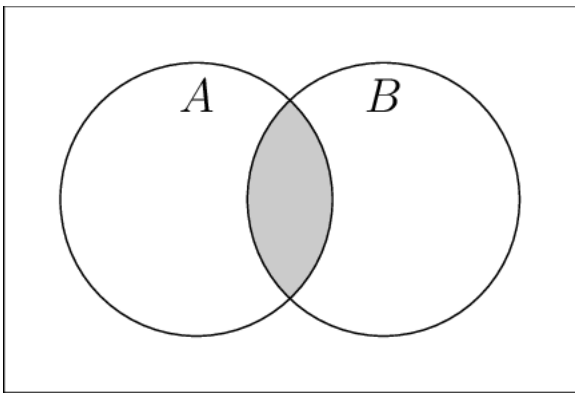
   Note: This is equivalent to asking how many surjective functions there are from a domain of size k to a codomain of size n.

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.

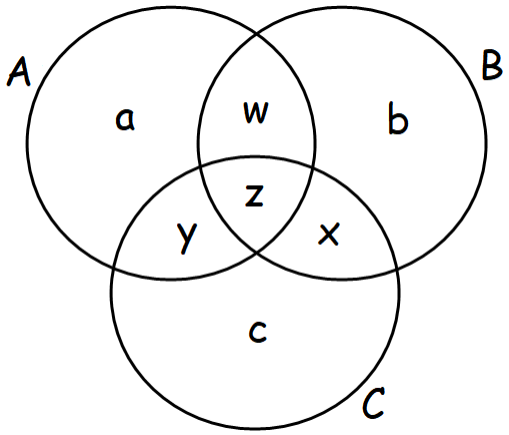
For instance, if $A = \{1, 2\}$ and $B = \{1, 3\}$, then $A \cup B = \{1, 2, 3\}$. $|A \cup B| = 3$, but $|A| + |B| = 2 + 2 = 4$. The problem is that we've double counted the elements that are in both A and B, that is, element 1. To fix this problem, we should subtract $|A \cap B|$.



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?

Solution:

w, x, y get double counted and z gets triple counted.

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

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

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

   Solution:
   Treat 24 as a single units, so we're left with permuting {1, 3, 5, 24}. There are 4! permutations.

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

   Solution:
   Same as above, 4!.

b. 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?

   Solution:
   Each of the 8 elements in X have two options of where to map to: b or c. So, it's $2^8 = 256$.

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

   Solution:
   There's only 1 option, so it's $1^8 = 1$.

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.

Solution:

Let the set of functions not mapping to a be A, not mapping to b be B, and not mapping to c be C.
$|A| = |B| = |C| = 2^8$, as established above, since the argument for i can be made to all three sets.
$|A \cap B| = |B \cap C| = |A \cap C| = 1$, as the argument for ii can also be generalized.
$A \cap B \cap C$ is functions from X to $\{\}$, which is no functions.
The total number of non-surjective functions is $|A \cup B \cup C| = 3 * 2^8 - 3 * 1 + 0 = 765$.

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

c. 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?

> **Solution:**
>
> We are asking what the size of the domain of a function needs to be, where the function is from socks to types, such that there is some style with at least 2 socks that map to it. The answer is therefore 5.

d. 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?

   > **Solution:**
   >
   > $n - 1$, dancing with everyone else

   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.)

   > **Solution:**
   >
   > The possible number of dance partners are $[0, n-1]$. Trying to apply the pigeonhole principle directly doesn't work, since it seems like all n astronauts could have all n possible numbers of partners. But, if someone has 0 dance partners, then no one can have $n-1$. So, the choices are either $[1, n-1]$ or $[0, n-2]$, each of which results in $n-1$ possible options for the number of dance partners. Since we have n astronauts, two people must have the same number of partners.

e. 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.

Solution:

Consider the differences $a_{n+1} - a_1$ .... $a_{n+1} - a_n$. If one of these differences has a remainder of 0 mod n, we are done. Otherwise, two of them have the same remainder: $a_{n+1} - a_i$ and $a_{n+1} - a_j$ where $i \neq j$. Subtract them from each other, and we are done.

f. *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.

Solution:

Partition the square into 4 unit squares. Then, there is a square with two dots. The maximum distance between two points within a unit square is square root of 2.

Checkoff - Call over a TA