Modular Arithmetic and Cryptography!

Math Circle Thursday January 22, 2015

What is Modular Arithmetic?

In modular arithmetic, we select an integer, n, to be our "modulus". Then our system of numbers only includes the numbers 0, 1, 2, 3, ..., n-1. In order to have arithmetic make sense, we have the numbers "wrap around" once they reach n.

Example: If we pick the modulus 5, then our solutions are required to be in the set {0, 1, 2, 3, 4}. We have 2+1=3 and 2+2=4 as usual. Then 2+3=5, which is not in our set, so it wraps around giving 2+3=0. Then 2+4=6, which wraps around to be 1.

This may seem strange, but in fact we use it everyday! Consider a clock, we go from 1 o'clock to 2 o'clock, ..., 11 o'clock, 12 o'clock, then back to 1 o'clock, and so on. This is an example of when the modulus is 12 and for clocks we use {1, 2, ..., 12} instead of {0,1, ..., 11}, but these are the same because we consider 0 and 12 to be the same in terms of wrapping around.

How do we write modular arithmetic?

Continuing the example above with modulus 5, we write:

$2+1 = 3 \pmod 5 = 3$

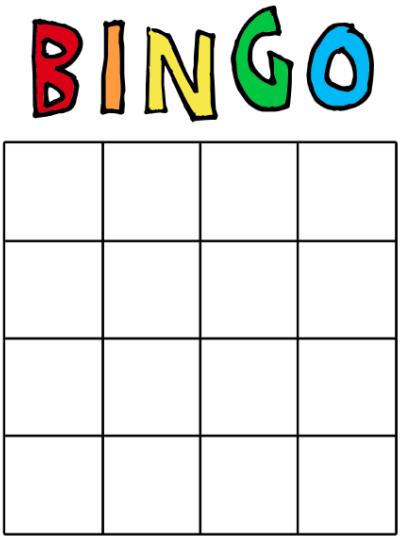
$2+2 = 4 \pmod 5 = 4$

$2+3 = 5 \pmod 5 = 0$

$2+4 = 6 \pmod 5 = 1$

Challenge question! What is 134 (mod 5)?

It might help us to think about modular arithmetic as the remainder when we divide by the modulus. For example 214 (mod 5) = 4 since $\frac{214}{5} = 42$ with remainder 4 (because $\frac{214}{5} =$ 42*5 +4).



Using the Caesar Cipher:
Line up the wheels so that the "a" lines up with "D". Now hold the wheel so that it doesn't turn. Convert the ciphertext into plaintext using the wheel to solve the following riddle!
Riddle: What do you get if you divide the circumference of a jack-o-lantern by its diameter?
Answer: SXPSNLQ SL

Now line up with wheels so that "a" lines up with "R".
Riddle:Why was the math book sad?
Answer: ZK YRU KFF DREP GIFSCVDJ

What if you find a secret message on the floor, and you don't know the "key" of how to turn the wheel? Can you still crack the secret message? Give it a try!

Hint: If you see a one letter word, what could it be?
Secret Message: Q VQHCUH YD JXU VYUBT MYJX XYI SEMI SEKDJUT DYDUJO EV JXUC, RKJ MXUD XU HEKDTUT JXUC KF XU XQT EDU XKDTHUT.

Secret Message: YJIJUUNU URWNB QJEN BX VDLQ RW LXVVXW. RC'B J BQJVN CQNH'UU WNENA VNNC.

Secret Message: YMWJJ TZY TK YBT UJTUQJ XYWZLLQJ BNYM KWFHYNTSX.

It's time to put our cryptography skills to use!

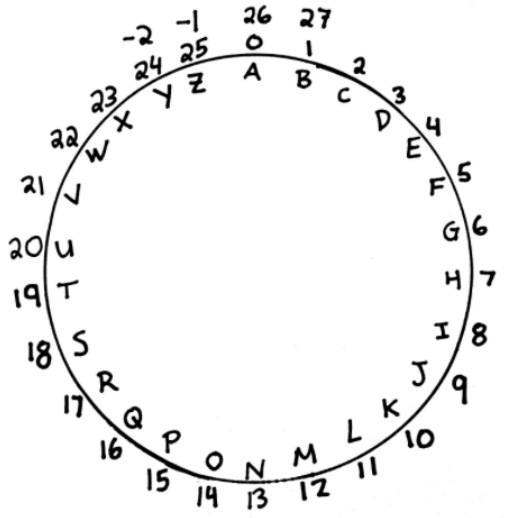
We will split everyone into two teams. Each person will write down the name of your favorite type of candy or candy bar. Then you will encrypt it picking a shift of the wheel, so if you pick "nerds" and a shift of lining up "a" and "B" then n→O, e→F, etc. Don't say your candy type out loud and don't tell anyone your shift! Once everyone has encoded their favorite type of candy, the two teams will switch and whichever team decrypts all the candy types fastest wins some real candy!

You can fill out the lines below if it helps you encrypt your candy name, but don't let the other team see it!

Candy name:
Line up the wheels so that the lowercase letter _____ lines up with the capital letter _____.
Encrypted candy name:

How do Modular Arithmetic and Caesar Ciphers relate?

Since there are 26 letters in the English alphabet, let's relate the letters a-z by numbers 0-25 as shown by the diagram below.



Notice going from "a" to "D" was a shift of 3 letters over. Thus we can encrypt the word "pumpkin" by relating "p" with 15 on the wheel, adding 3 to get 18, and then we turn this back into a letter, which gives us "S". Similarly "u" $\rightarrow$ 20 $\rightarrow$ 23 $\rightarrow$ X.

Challenge Questions!

1) What number did we "add" in the second riddle to encrypt the message?

2) If adding 3 took us from the plaintext to the ciphertext, what do you think we would do to go from the ciphertext back to the plaintext?

3) How many different ways can you encrypt a message using a Caesar cipher? Hint: What does "adding" 26 do?

4) From your experience cracking the secret messages do you think it is relatively easy or hard to test all combinations to crack someone's secret message?

5) Can you think of something we could do to make secret messages more secure?

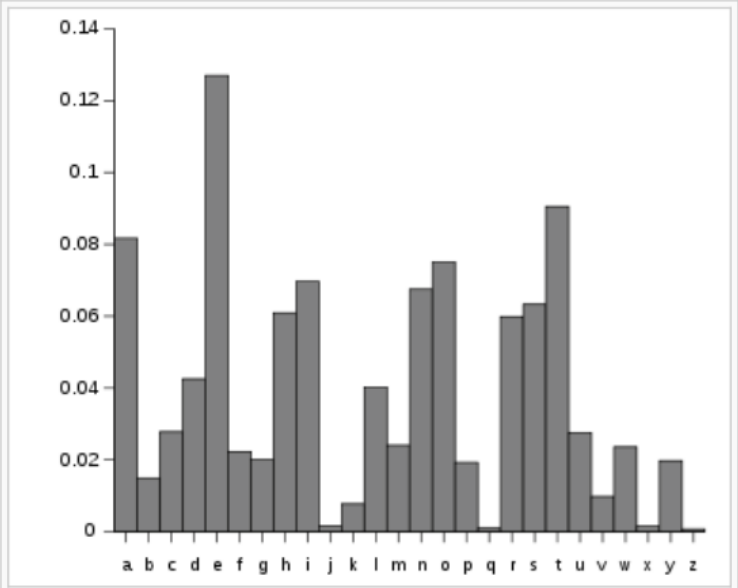
TOP SECRET: Don't read unless you've studied the Caesar cipher!

How to Crack the Caesar Cipher:

As we've discovered, there are only 25 different shifts we can use to encrypt a message with a Caesar cipher. Because of this, the Caesar cipher is considered to be a very weak type of cryptography. We call the act of testing all 25 options until finding the key, the method of **brute force**.

However, even if we couldn't use brute force the Caesar cipher is still considered to be weak. This is because each letter of the alphabet (say "a") always gets encrypted to the same letter (which depends on your shift). Also two different letters cannot go to the same letter (meaning we cannot send "a" to "N" and send "b" to "N". Because of this one-to-one correspondence, another method of cracking the Caesar cipher is with **frequency analysis**.

In the English language, the most common letter is "e" which occurs 12.7% of the time! This means that on average every 8th letter in a sentence is an "e". Just look at that last sentence and notice how many "e"'s were in it! The second most common letter is "t" which occurs 9.1% of the time. The third most common letter is "a" which occurs 8.2% of the time. The frequencies of each letter are shown below.



Relative frequencies of letters in text.

The way to use frequency analysis to break the Caesar cipher is as follows. First count of the number of "A"'s in the ciphertext, the number of "B"'s in the ciphertext, the number of "C"'s, etc. Then when you plot those values on a graph, you should see the same pattern of spikes, but shifted in a different position. This will be the shift or "key" to the Caesar cipher! It's important to note that this method is not good for short ciphertexts (such as a single word) because the frequencies of a short text could be off. Also this method is not full-proof: there is a book *Gadsby* by Ernest Vincen Wright that does not contain the letter "e" (think of how much work writing that book must have been!).

The Vigenère Cipher

A major weakness of the Caesar cipher is that there are not many ways to encrypt a message. Also long messages encrypted with the Caesar cipher are easily cracked using "frequency analysis". A stronger cipher is the Vigenère cipher. Here's how it works!

1) Pick any small integer (say 3). This will be the "key length"
2) Now since we chose 3 above, we need to pick 3 different numbers to be our shifts (say shift 2, shift 9, and shift 21).
3) We encode our secret message by shifting the 1st, 4th, 7th, ... letters by 2. The 2nd, 5th, 8th, ... letters we shift by 9. And the 3rd, 6th, 9th ... letters we shift by 21.

For example: Encrypting the word "pineapple" we have:
"p"$\rightarrow$ 15 $\rightarrow$ 17 $\rightarrow$ "R"
"i"$\rightarrow$ 8 $\rightarrow$ 17 $\rightarrow$ "R"
"n"$\rightarrow$ 13 $\rightarrow$ 13+21 = 34 (mod 26) = 8 $\rightarrow$ "I"
"e"$\rightarrow$ 4 $\rightarrow$ 6 $\rightarrow$ "G"
"a"$\rightarrow$ 0 $\rightarrow$ 9 $\rightarrow$ "J"
"p"$\rightarrow$ 15 $\rightarrow$ 15+21=36 (mod 26) = 10 $\rightarrow$ "K"
"p"$\rightarrow$ 15 $\rightarrow$ 17 $\rightarrow$ "R"
"l"$\rightarrow$ 11 $\rightarrow$ 20 $\rightarrow$ "U"
"e"$\rightarrow$ 4 $\rightarrow$ 4+21=25 $\rightarrow$ "Z"
So "pineapple" became "RRIGJKRUZ".

Notice if we had picked the number 1 in the first step of the process we have the Caesar cipher!

Let's try it out!

One way people use the Vigenère cipher is to pick a short codeword, say "dog". This means your key length will be 3 because "dog" has 3 letters. It also means your first shift is d=3 on the wheel. Your second shift is o=14, and your third shift is g=6. These are the shifts that the person writing the secret message uses, so do decode the message you will subtract 6 from the 1st, 4th, 7th, etc letters, and so on.

One way to organize creating a Vigenère cipher is as follows:
1) Start with a blank grid with three rows:

2) Fill in the middle line with the message you'd like to encrypt:

I		l	o	v	e		m	a	t	h				

3) Pick your code word and write it on top (including the shifts these letters correspond to). Also convert your message letters to the corresponding numbers they represent:

C (+2)		A (+0)	R (+17)											
I 8		l 11	o 14	v 21	e 4		m 12	a 0	t 19	h 7				

4) Repeat the code across the top, then add down the numbers (mod 26) and convert those number back into letters:

C (+2)		A (+0)	R (+17)	C (+2)	A (+0)		R (+17)	C (+2)	A (+0)	R (+17)				
I 8		l 11	o 14	v 21	e 4		m 12	a 0	t 19	h 7				
10 K		11 L	31=5 F	23 X	4 E		29=3 D	2 C	19 T	24 Y				

You could use a similar system to decode Vigenère ciphers, using - instead of + for the codeword.

Let's try it out! Suppose we arranged our secret codeword to be "dog" and I sent you the secret message below. Try to decode it! I've started the table for you!

Secret Message: ZVE GCKV BUEBJB HGOY ZR QOUQRHG? HHQGXGK WVKUS OV BU SCOQH.

D (-3)	O (-14)	G (-6)											
Z (25)	V (21)	E (4)		G (6)	C (2)	K (10)	V (21)						

Now you try to create a secret message! Pick a codeword and encrypt your name (or any other secret message you'd like!) using the grids below to help guide you.

Trade with someone else and try to decrypt their name (or secret message). Make sure you ask them for the codeword!:

Challenge Questions!

1) How would you decrypt the Vigenère cipher used to encrypt "pineapple"?

2) In general, if your friend said they encrypted a Vingenère cipher using the key (5,11,1, 2), how would you decrypt their ciphertext?

3) If you pick the integer 3 in the first step of the Vigenère process, how many different ways could you encrypt a message? What if you pick the integer 5?

4) In the Caesar cipher, the same letter always got turned into the same letter (for example the "p" in pumpkin always turned into an "S". Does this happen in the Vigenère cipher? Hint: look at what happened to "pineapple".

5) Also in the Caesar cipher you could not encrypt two different letters to be the same letter (meaning if "p" $\rightarrow$ "S" then nothing else can go to "S"). Is this true of the Vigenère cipher too? Hint: again look at what happened to "pineapple".

6) Is this more or less secure than the Caesar cipher? By a little or a lot?

Extreme Challenge Question!

In the Caesar cipher and Vigenère cipher we encrypted the words by adding to the value of the letter (mod 26). And thus we could decrypt by subtracting that value (mod 26). Now instead of adding (mod 26), could we use multiplication (mod 26)? Well it's certainly easy to say "sure multiply by 3 then take the answer modulo 26", but then how would you decrypt? What would it mean to "divide" (mod 26)?