LAMC Junior Circle:
Modular Arithmetic and Ciphers

Preston Carroll

June 3, 2018

1. **Warmup:**
   The Caesar cipher is a cipher in which every letter is shifted by a constant amount. For example, if I represent the word "CAB" with numbers it would be "2 0 1". Then, I would pick a number to shift all these numbers by; in our case let's shift it by 3. This means my new message or ciphertext will be "5 3 4". This is the same as "FDE". In order to decode this my partner would need to reverse this shift, that is, they would need to shift each of the letters by -3 to recover the word "CAB".

   Let's try this with an example. The ciphertext of a message is provided below. The shift is +1:

   Ciphertext: qmfbtf ipme vq uif ovncfs uisff xifo zpv bsf epof.

   Plaintext:

2. A powerful mathematical tool when working with ciphers is modular arithmetic. Modular arithmetic is similar to how we tell the time. For example, if it is 3PM right now, what time was it 4 hours ago? We do not say that it was -1PM, rather we say that it was 11AM. The way to deal with this mathematically is to write:

   $$3 - 4 \ \textit{modulo} \ 12 = 11$$

   The way to perform this calculation is very similar to division, except we are only interested in the remainder. So in the case of 31 *mod* 26 we would find that $\frac{31}{26} = 1$ remainder 5, and so

   $$31 \ \textit{mod} \ 26 = 5$$

   Let's try this with some examples. Patterns are very important in these type of problems and can make these calculations *much* easier to perform, so try to find some!

   (a) 5 mod 26 =

(b) 71 mod 70 =

(c) 101 mod 101 =

(d) Googolplex mod 2 =

(e) 52 mod 20 =

(f) 2018 mod 1000 =

(g) 408 mod 7 =

(h) 36972 mod 3 =

3. We can apply this concept of modular arithmetic to more easily encrypt and decrypt our messages. Using your alphabet table, encrypt the following three messages with 3 different shifts of your choosing. One of them has been started for you.

   (a) Ciphers are fun

   Your shift: +1

Plaintext	c	i	p	h	e	r	s		a	r	e		f	u	n
Numbers	2	8	15	7	4	17	18		0	17	4		5	20	13
Shifted Numbers	3	9	16	8	5	18	19		1	18	5		6	21	14
Ciphertext															

   (b) Squircles are the best

   Your shift:

Plaintext	s	q	u	i	r	c	l	e	s		a	r	e		t	h	e		b	e	s	t
Numbers																						
Shifted Numbers																						
Ciphertext																						

   (c) Dodecahedron

   Your shift:

Plaintext	d	o	d	e	c	a	h	e	d	r	o	n
Numbers												
Shifted Numbers												
Ciphertext												

4. Inverses of Numbers

(a) What is an inverse? If we have a number a, for example, and we want to find a^{-1}, we are really looking for the number such that when I multiply it by a, we get 1.

$$a \cdot a^{-1} = 1$$

So say I have 10. What is the inverse of 10? Well let's look at our definition, what number, when I multiply it by 10, do I get 1? That number is exactly $\frac{1}{10}$! Inverses in regular arithmetic are quite easy to find. Commonly we write the inverse of a number in the form of a^{-1}. So for if I am talking about the inverse of 10, I can write it as 10^{-1}, but to evaluate it I would write it as $\frac{1}{10}$

i. $2^{-1} =$

ii. $13^{-1} =$

iii. $\pi^{-1} =$

iv. $1^{-1} =$

(b) How is an inverse different with modular arithmetic? In actuality, inverses are the same in that they follow from the same definition, but finding them is generally more difficult to do by hand. Let's try and find the inverse of 9 modulo 26. We'd write this as

$$9^{-1} \ mod \ 26$$

Looking back the definition of an inverse, we want to find a number such that when I multiply it by 9, I get 1. Keep in mind that we do have this extra step of doing our modular arithmetic and that we are only able to use whole numbers between 1 and 25. What is $1 \cdot 9$ mod 26, well it is just 9, so 1 is not the inverse of 9 in mod 26. How about 2? $2 \cdot 9$ mod $26 = 18$ mod 26. No luck again, let's try one more time. $3 \cdot 9 = 27$ mod $26 = 1$ mod 26. Voila! 3 is the inverse of 9 mod 26, because when I multiply 3 by 9 in mod 26 I get 1.

(c) Try and find the inverse of 7 in mod 17.

$$7^{-1} \ mod \ 17 =$$

5. Introduction to Affine Ciphers:
   Affine ciphers are very similar to the Caesar cipher with an extra twist. Rather than just adding one specific number to each letter in our message, we first multiply it by some number (mod 26) and then we add a number.

   (a) Let's explore this with an example:

   - Let's say we had the message "Hello World" which is "07-04-11-11-14 22-14-17-11-03" in numbers.
   - Then we would pick a secret α and β. Our α is the number we will multiply by and β is the number we will add. I will pick $\alpha = 21$ and $\beta = 3$.
   - To encode my message I will first do the modular multiplication so my first letter H, which is a 7, becomes $21 \cdot 7 = 147 \bmod 26 = 17 \bmod 26$.
   - Then I will add my β of 3, so I add 3 to 17 to get 20 as the first letter of my cipher text (the letter U).
   - If I continue this procedure for each letter I will get the ciphertext of: "UJAAL XLWAO"

   (b) So how does this relate to modular inverses? Well, encryption seems pretty simple to perform if we know what α and β we want. But what about *decryption*? To perform the decryption we will need to reverse our modular multiplication by multiplying by the modular inverse. Let's pretend for a moment that we didn't know what the original plaintext was, and that we only had the ciphertext, α, and β. How do we go backwards? Well let's first take the letter U, convert it into its number form of 20, then subtract three. Now we have the number 17. All we know is that someone had a number, and then multiplied it by 21 in modulo 26 and got 17. To reverse this we can just use the modular inverse of 21! With some trial and error we can pretty quickly find that 5 is the inverse of 21 in mod 26. So we can just multiply 17 by 5 in mod 26 and get our original letter. $5 \cdot 17 \bmod 26 = 85 \bmod 26 = 7 \bmod 26$. 7 is the number for H and we are done! To review:

$$Ciphertext = \alpha(Plaintext) \ + \beta \ (mod \ 26)$$

$$Ciphertext - \beta = \alpha(Plaintext) \ (mod \ 26)$$

$$\alpha^{-1}(Ciphertext - \beta) = Plaintext \ (mod \ 26)$$

   - Subtract β from the ciphertext
   - Find the modular inverse of α and then multiply that by the number you obtained by subtracting β
   - Convert back into letters.

$$Ciphertext = \alpha(Plaintext) \ + \beta \ (mod \ 26)$$

$$20 = 21 \cdot (Plaintext) \ + 3 \ (mod \ 26)$$

$$20 - 3 = 21 \cdot (Plaintext) \ (mod \ 26)$$

$$5(17) = (Plaintext) \ (mod \ 26)$$

$$85 = (Plaintext) \ (mod \ 26)$$

$$7 \ (mod \ 26) = H$$

(c) Homework: Perform a decryption of the following ciphertext:
(Hint α=9, β=3)
Ciphertext: xs xj hbvo odaena sz envalis soxj xjq's xs?

6. Which cipher is easier to work with?

7. Which cipher is better to hide secrets from someone who can see your ciphertext, but does not know your key?