CMI Math Circle

Synopsis for August 9 2026

In this session we continued our exploration of ciphers. We explored two properties of the shift cipher, namely:

1. How many different shift ciphers are there?
2. Will a sequence of shifts make the shift cipher any stronger?

We did not introduce modular arithmetic yet, and based the discussion on language that students already know. Most students could figure out that the phrase *remainder after division by 26* is coming up quite often.

Some explorations we used:

1. Encrypt the word

   `SAFETY`

   using each of the following shifts. What do you notice?

Shift	Ciphertext
$+3$	
$+29$	
-23	

2. Without encrypting the message, predict the answers.
   (a) Is shifting by 15 the same as shifting by 41?
   (b) Is shifting by 7 the same as shifting by -19?
   (c) Is shifting by 24 the same as shifting by -2?

3. Complete the table.

Shift	Equivalent shift between 0 and 25
29	
41	
-3	
-11	
53	
-52	

What conclusion can you draw?

4. How many different shift ciphers are possible? Explain your reasoning.

5. Encrypt the word

   SECRET

   1. Shift by 5.
   2. Shift the result again by 7.
   3. Now encrypt the original word directly by shifting by 12.

   Are the two ciphertexts the same?

6. For each pair of shifts, determine the single equivalent shift.

Two shifts	Equivalent single shift
$10,\ 18$	
$-14,\ 15$	
$20,\ 10$	

7. Can you explain why applying several shift ciphers never makes the encryption stronger?

Next we proceeded to the the encryption scheme $x \mapsto ax$, where a is the 'key', which was introduced last time. This week we took the exploration ahead trying to see if we can figure out which keys work and which don't for inverting the cipher.

While some students could work through the entire worksheet, we found that a number of students had difficulties grasping the concept of emphinverting the operation in this way, since everything was happening module 26. While they could understand what the end goal was, a number of them could not figure out by themselves how to get there.

We had ended the previous session with the following question:

Suppose the encryption multiplies every letter by 3*. Can you find a number that reverses this operation?*

Such a number will be called the the "multiplicative inverse of 3".

Recalling what was observed:

Plaintext letter	Plaintext number x	$3x$, ciphertext letter	$9 \times 3x$, decrypted letter
A	0	0, A	0, A
B	1	3, D	27, B
C	2	6,	
D	3	9,	
O			
S			
T			
Z			

We can record our observation as:

If the encoding is done by multiplying the plaintext number by 3*, then decoding can be done by multiplying the ciphertext number by* ____.
In short, multiplication by ____ *reverses the multiplication by* 3.

3 and 9 can be called 'inverses' of each other in this context.

Next we encouraged students to work using the same logic to see if we can find inverses for other integers between 0 and 26 by completing the following table:

n	Inverse of n?		n	Inverse of n?		n	Inverse of n?	
0			9			18		
1			10			19		
2			11			20		
3			12			21		
4			13			22		
5			14			23		
6			15			24		
7			16			25		
8			17					

The following explanation helped some students understand that two integers m and n would be inverses if $m \times n$ leaves remainder 1 when divided by 26.

Suppose we want to find the inverse m, and n is such that mn leaves every plaintext letter fixed (as 3×9 does). This means if x is any plaintext number, then

$$mnx \;=\; 26k + x \quad \text{for some integer } k$$

In particular, for $x = 1$, $mn = 26k + 1$. So n satisfies the property that mn leaves remainder 1 when divided by 26.

There were few students who found that inverses will not exist for even integers, since these never give remainder 1 when divided by 26. Most students, with some explanation and help, could figure out the remaining inverses.

Some students who were familiar with it, tried to frame this problem using modular arithmetic.

Overall, the idea turned out to be more challenging for the students than expected.