RAM Math Circle - Chennai

Session Report - February 2 2025

1 Geometry

In the previous session we worked on proving that in any triangle, the following segments concur at a point -

1. the perpendicular bisectors of three sides of a triangle
2. the bisectors of the three angles of a triangle

Now we will continue in the same vein and prove the following -

1. In any triangle, the following segments meet (or concur) at a point:
   (a) the three medians of a triangle
   (b) the three altitudes of a triangle

.

2 Cryptography

In earlier sessions we have studied the shift cipher. In this session we will study one more cipher called the *affine cipher*.

We will use the following encoding for the English alphabet to create as well as decipher our codes:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

Recall the following terms: -

- ***Encryption*:** the process of converting plaintext to coded form (or ciphertext).
- ***Decryption*:** this is the opposite of encryption, that is, its the process of converting ciphertext back to plaintext so everyone can understand it.
- ***Key*:** this is the number used to perform the encryption process.

For affine ciphers, the encryption function is defined as follows: fix two integers a and b and define

$$E_{a,b}(x) = ax + b.$$

This means the encryption key is the pair of numbers a, b.

Examples:

1. Encrypt the plaintext ‘cryptography is cool’ with the key pair $(3, 7)$.
2. Encrypt the plaintext ‘this is the message’ with the key $(-5, 2)$.

In order to find a decryption formula for an affine cipher, we have to think about how the encryption can be reversed. Since the term b is added in encryption, it should be subtracted in decryption. However, reversing the effect of multiplication by a takes some work.

From the properties of multiplication in real numbers, we know that $n \times \frac{1}{n} = 1$. So the effect of multiplying by an integer k can be undone by multiplying with $\frac{1}{k}$. For example, if $2x = 5$, then $\frac{1}{2} \times 2x = \frac{1}{2} \times 5$ gives us $x = \frac{5}{2}$.

When we are working entirely in the set of integers modulo n, we do not have fractions or reciprocals to work with. In this case we need an analogue of reciprocals that will ‘undo’ the effect of multiplying by an integer a. We call this analogue the *multiplicative inverse of a modulo n*. It turns out that the existence of such an inverse depends on the relation between a and n.

Let us calculate the multiplicative inverses modulo n for some small values and n and see if we can make an observation about the general pattern.

1. Calculate the multiplicative inverses modulo n for each of the cases $n = 5, 6, 7$ and 8.
2. Make a conjecture about the existence of multiplicative inverses modulo n.
3. Make a list of all numbers from 0 to 25 which have a multiplicative inverse modulo 26, along with their inverses.
4. What should be the decryption key for the affine cipher if the encryption key is (a, b)?
5. Decrypt the ciphertext ‘Jtuq mct rxutb’ using the decryption key $(9, 7)$.
6. Decrypt the ciphertext ‘GWNSL YMJ ITHZRJSYX’ given that the encryption key is $(1, 5)$.
7. Decrypt the ciphertext ‘BRUY YRMEDF ZI IWYQ’ given that the encryption key is $(3, -4)$.