IMSc - RAM Math Circle - Chennai

Synopsis for August 16, 2026

In this session we worked on bringing the walking-around-polygons investigation to a natural conclusion. The main goals were:

- to consolidate the observation that a walk with step size k is complete precisely when k is relatively prime to n;
- to investigate the relationship between a walk and the same walk performed backwards;
- to notice that complete walks occur in pairs;
- to move from finding successful step sizes to *counting* them;
- to introduce Euler's totient function $\varphi(n)$ as a name for this naturally occurring count.

After this exploration, we introduced shift ciphers through another worksheet. The aim was to give the children a second, quite different setting in which the same "wrap-around" behaviour appears.

We used 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

Then we introduced some terms which were going to be used in this exploration:

- ***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.

Examples

1. Encrypt the plaintext 'cryptography is cool' with the key 7.
2. Encrypt the plaintext 'this is the message' with the key -5.
3. Decrypt the ciphertext 'WIRH XLI QSRIC' using the key -4.
4. Decrypt the ciphertext 'YMNX NX JFXD' using the key -5.
5. Decrypt the ciphertext 'XYFD XFKJ JSJRD PSTBX' by working out the key.