CIFRARIO DI CESARE E CONGRUENZE

Vogliamo schematizzare un alfabeto cifrante:

Numeriamo le 21 lettere dell'alfabeto da 0 a 20

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

Decidiamo che la nostra chiave sia 5 e lo sommiamo ad ogni posizione così da ottenere che nell'alfabeto cifrante la A occuperà il posto 5 cioè corrisponde alla F, la B alla G,….. la S che occupa la posizione 16 corrisponde alla A, la lettera T alla B. Vediamo il ragionamento matematico:

17+5=22, ma dato che le posizioni possibili sono 20 e sono numerate da 0 a 20, 22=1·21+1 la T corrisponderà alla posizione 1 cioè B.

18+5=23=1· $21 + 2$, la U occuperà il posto 2 che è C e così via.

In matematica questo tipo di calcoli rientrano nell'aritmetica modulare o aritmetica dell'orologio. Il primo a ideare questa aritmetica fu Gauss.

Definizione: $sia\ n\ un\ intero\ positivo\ fissati, a\ e\ b\ due\ interi\ si\ dice\ che\ a \equiv b\ mod n \leftrightarrow a - b$ è $multiplo\ di\ n.$

Esempi $25 \equiv 1 mod 3\ perche\ 25 - 1 = 24\ che$ è $multiplo\ di\ 3$

$$-5 \equiv 1 mod 6\ perch\text{è}\ -5 - 1 = -6\ che\ \text{è}\ multiplo\ di\ 6$$

Allora come nell'orologio delle ore il 15 corrisponde a 3 e quindi $15 \equiv 3\ mod\ 12\ perch\text{è}\ 15 - 3 = 12, multiplo\ di\ 12$.

Questa relazione equivale a dire che 15 diviso 12 dà come resto 3, anche 39 diviso 12 dà come resto, 27 diviso 12 da come resto 3, anche -33 diviso 12 da come resto 3 (quoziente 3). Allora tutti i numeri divisi per 12 possono dare come resto 0, oppure 1,(2,3,4,5,6,7,8,9,10,11). Si formano degli insiemi i cui elementi sono i numeri che divisi per n danno lo stesso resto. Tali insiemi si chiamano classi di resto modulo 12.

Tutti gli insiemi si indicano con il numero rappresentante tra parentesi quadre, esempio [0] è l'insieme dei numeri che divisi per 12 danno come resto 0. La classe di tutti questi numeri prende il nome di Z_{12}.

Attività: costruire degli orologi di Gauss con n=3,4,5.