III LEZIONE
(note tratte dalle lezioni 1 e 2 del laboratorio di Crittografia, scritte da Evangelista, Testa e Tuzzolo nell'ambito del corso di perfezionamento
http://www.mat.uniroma2.it/pls/corsop/doc.html
alla voce "Laboratori proposti dai corsisti", laboratorio "Numeri primi e crittografia")
La cifratura di Cesare suggerisce l'utilizzo delle congruenze.

DEF. Sia *n* un intero positivo fissato. Due numeri $a, b \in Z$ sono ***congrui modulo n*** se e solo se a-b è un multiplo di n, ovvero, espresso in formule, $a \equiv b \ \ (n) \Leftrightarrow (a-b) = n \cdot h$ per qualche $h \in Z$.

Esempi:

1. $25 \equiv 1 \ \ (3)$ perché $25 - 1 = 24 = 3 \cdot \mathbf{8}$
2. $67 \equiv 55 \ \ (6)$ perché $67 - 55 = 12 = 6 \cdot \mathbf{2}$
3. $55 \equiv 1 \ \ (6)$ perché $55 - 1 = 54 = 6 \cdot \mathbf{9}$
4. $-5 \equiv 1 \ \ (6)$ perché $-5 - 1 = 6 \cdot \mathbf{1}$

Fissato n, tutti i numeri 0,….,n-1 siano in un certo senso speciali in quanto un qualsiasi altro numero intero (positivo o negativo) sarà congruo ad uno di essi modulo n.
Questo ruolo speciale sta proprio nel fatto che scelto un qualsiasi b tale che $0 \le b \le n-1$ tutti gli altri numeri interi il cui resto della divisione per n è uguale a b possono essere identificati con b stesso nel senso della congruenza.

Restano così definiti n insiemi di numeri ovvero:

DEF. Gli insiemi della forma $\overline{b} = \{a \in Z \mid a \equiv b(n)\}$= interi che divisi per n danno resto b si chiamano ***classi di resto modulo n***. I numeri b sono tali che $0 \le b \le n-1$ e vengono chiamati ***rappresentanti della classe***.

ESEMPIO Possiamo calcolare tutte le classi di resto modulo 4:
$\overline{0} = \{....,-16,-12,-8,-4,0,4,8,12,....\}$= interi che divisi per 4 danno resto 0
$\overline{1} = \{..,-11,-7,-3,1,5,9,....\}$= interi che divisi per 4 danno resto 1
$\overline{2} = \{...,-6,-2,2,6,10,...\}$= interi che divisi per 4 danno resto 2
$\overline{3} = \{..,-9,-5,-1,3,7,11,....\}$ = interi che divisi per 4 danno resto 3.

DEF. L'insieme di queste classi di numeri si indica con Z_n. Cioè $Z_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Proprio come in Z, vi si possono definire operazioni che ci consentono di trattare le classi si resto quasi come numeri interi. E' possibile definire somma, prodotto e creare tutta un'aritmetica che viene definita aritmetica modulare perché si lavora modulo n (nel senso delle congruenze).

DEF. Date $\overline{a}$ $\overline{b}$ due classi di resto modulo n si ha che:

- $\overline{a} + \overline{b} = \overline{a+b}$
- $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Per comodità di calcolo esprimeremo il risultato di queste operazioni sempre tramite il suo rappresentante cioè se, ad esempio, stiamo lavorando modulo 5 e dobbiamo calcolare la somma tra $\overline{3}$ e $\overline{4}$ faremo $\overline{3} + \overline{4} = \overline{7} = \overline{2}$ poiché $7 \equiv 2 \ \ (5)$ e similmente per il prodotto.

Osserviamo che la definizione di queste di queste operazioni è ben posta cioè è indipendente dal rappresentante della classe che si sceglie per operare. Inoltre, le operazioni cosi' definite sono commutative e associative. Entrambe sono dotate di elemento neutro; infatti:

$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$

$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$

e ogni elemento ammette opposto rispetto alla somma.

La somma viene descritta per prima nell'ambito del laboratorio. Essa permette di rivedere la cifratura di Cesare.

Riassumendo in una tabella l'associazione lettera-numero fatta precedentemente,

Lettera	Numero	Lettera	Numero	Lettera	Numero
a	0	h	7	q	14
b	1	i	8	r	15
c	2	l	9	s	16
d	3	m	10	t	17
e	4	n	11	u	18
f	5	o	12	v	19
g	6	p	13	z	20

possiamo notare che l'alfabeto numerico dei messaggi unitari (le singole lettere) è rappresentato da $P = Z_{21}$.

Poiché nel cifrario di Cesare ogni lettera viene sostituita con la lettera che si trova un certo numero di posizioni più avanti abbiamo che l'insieme delle chiavi è $K=\{0,1,...,20\}$.

Il sistema crittografico per traslazione può essere cosi schematizzato:

data la chiave $k \in K$, la funzione cifrante sarà la seguente:

$C_k : Z_{21} \to Z_{21}$

$p \to p + k \mod 21,$

mentre la funzione inversa, quella di decifratura, sarà:

$D_k : Z_{21} \to Z_{21}$

$c \to c - k \mod 21.$

Giocando con le operazioni in Z_n, e' possibile cercare altre cifrature: cosa succede se ,per cifrare, moltiplico per un elemento fissato? Sto considerando l'applicazione: $Z_n \to Z_n$ definita da: $x \mapsto ax$.

Cosa succede se, per cifrare, elevo ogni elemento ad una potenza fissata? Sto considerando l'applicazione: $Z_n \to Z_n$ definita da: $x \mapsto x^t$.

Sono trasformazioni accettabili come cifrature? I ragazzi comprendono facilmente che una cifratura deve necessariamente essere una applicazione iniettiva. Poiche' dominio e codominio sono lo stesso insieme finito, una applicazione è iniettiva se e solo se è suriettiva se e solo se è biiettiva.

La prima idea (usare, come operazione di cifratura la moltiplicazione per un numero fissato a) non funziona sempre: ad esempio, modulo 9, la moltiplicazione per 3 non è iniettiva, e dunque non è una operazione di cifratura:

$3 \cdot 5 \equiv 3 \cdot 8 \equiv 6 \ (9)$ ma non è vero che $5 \equiv 8 \ (9)$.

La legge di cancellazione $a \cdot b = a \cdot c \Rightarrow b = c$ che vale in Z purché sia $a \neq 0$ non si trasporta dunque alle congruenze. Sperimentando su casi specifici, i ragazzi riflettono sulla definizione di applicazione iniettiva e suriettiva e sono portati a indovinare la caratterizzazione di numeri "buoni" da usare, per assicurarsi che la moltiplicazione per essi sia iniettiva (e automaticamente suriettiva): *se lavoro modulo n, la moltiplicazione per a definisce una funzione di cifratura se e solo se MCD(a,n)=1*.

Un lato della dimostrazione di questo fatto è più semplice: sicuramente se $MCD(a,n)=d>1$ si ha che $a = d\,r$ e $n = d\,t$ per opportuni numeri interi r e t. Ma allora $a\,t = d\,r\,t = (d\,t)\,r = n\,r$ è congruente modulo n a $a\,0$. Per dimostrare il viceversa, vengono introdotti il metodo delle divisioni successive e l'identità di Bezout, riportati negli appunti della quarta lezione.