II INCONTRO

TAVOLA 2.1: ripasso sulle classi resto
Ricordiamo che

$$a \equiv b \bmod n \Leftrightarrow \bar{a} = \bar{b} \text{ in } \mathbf{Z}_n.$$

Utilizziamo, per comodità di scrittura, entrambi i simboli $\bar{a}$ e **[*a*]** per indicare una classe resto.

Abbiamo visto che il metodo di Cesare, che opera traslando, è facilmente attaccabile con l'analisi delle frequenze. Sapendo che un testo è stato cifrato con il metodo di Cesare, è possibile anche procedere per tentativi, cioè provando tutte le 20 chiavi possibili. Occorre dunque cercare un metodo di cifratura più efficace e sicuro.
Ricordiamo che considerando le lettere come elementi di $\mathbf{Z}_{21}$ possiamo modellizzare la procedura di cifratura di Cesare nel modo seguente:
data la chiave $k \in \mathbf{Z}_{21}$, la funzione cifrante è:

$$C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\bar{m} \mapsto \overline{m+k}$$

mentre la funzione inversa, quella di decifratura, è:

$$D_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\bar{c} \mapsto \overline{c-k}$$

La traslazione offre poche possibilità perché è un procedimento troppo semplice: tre lettere consecutive dell'alfabeto in chiaro (ad esempio *a*, *b*, *c*) vengono cifrate con tre le lettere consecutive dell'alfabeto cifrante (ad esempio D, E, F se la chiave è $k = 3$). Per rendere più efficace la cifratura, bisogna eliminare questa regolarità con cui si susseguono le lettere. Per farlo è necessario "complicare" la funzione di cifratura C_k.
Per migliorare il sistema crittografico occorre quindi che la funzione di cifratura segua un ordine apparentemente casuale, ma che almeno per noi e per il destinatario del nostro messaggio mantenga una logica ben precisa: *per praticità, se la cifratura si può effettuare secondo una regola semplice da memorizzare, è più facile non commettere errori.*
Per capire meglio come procedere riprendiamo lo studio dell'insieme $\mathbf{Z}_n$ delle classi resto modulo *n*. Proprio come in **Z**, vi si possono definire operazioni che ci consentono di trattare le classi resto come numeri. 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. Si definiscono due operazioni in $\mathbf{Z}_n$. Date due classi resto $\bar{a}$ e $\bar{b}$ modulo *n*, si pone:

- la somma di classi: $\bar{a} + \bar{b} = \overline{a+b}$
- il prodotto di classi: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Osserviamo che la definizione di queste operazioni è ben posta, cioè è indipendente dalla scelta del rappresentante della classe. Infatti, se $a \equiv a' \bmod n$ e $b \equiv b' \bmod n$, allora $a = a' + hn$ e $b = b' + kn$ per opportuni $h, k \in \mathbf{Z}$. Ma allora

$$a+b = (a' + hn) + (b' + kn) = a' + b' + (h+k)\, n$$

e dunque $a+b \equiv a'+b' \bmod n$ e la somma è ben definita.
Inoltre

$$a \cdot b = (a' + hn) \cdot (b' + kn) = a' \cdot b' + (hb' + ka' + n)\, n$$

e dunque $a \cdot b \equiv a' \cdot b' \bmod n$ e il prodotto è ben definito.
Ad esempio: $[18]+[21] = [3] \bmod 4$: infatti $18+21 = 39$ e $[39] = [3] \bmod 4$ perché $39 = 4*9+3$.
D'altronde, $[18] = [2]$ (perché $18 = 4*4+2$) e $[21] = [1]$ perché $21 = 4*5 + 1$: utilizzando i nuovi rappresentanti trovo lo stesso risultato, perché $[2+1] = [3]$.

Lo stesso vale per il prodotto: [17] * [10] = [170] = [2] mod 6. D'altronde [17]=[5] mod 6 e [10]=[4] mod 6: potevo dunque scrivere [5] * [4] = [20] = [2] mod 6.

TAVOLA 2.2 : tabella del prodotto per $n = 5, 6, 9$.

Osserviamo che valgono le proprietà associativa e commutativa per la somma e per il prodotto; vale anche la proprietà distributiva della somma rispetto al prodotto.
Inoltre, entrambe le operazioni definite sono dotate di un elemento particolare, analoghi dello 0 e dell'1 in $\mathbf{Z}$: infatti, preso un qualsiasi elemento $\bar{a} \in \mathbf{Z}_n$ vale che:

$$\bar{a} + \bar{0} = \bar{a}$$
$$\bar{a} \cdot \bar{1} = \bar{a} \quad .$$

Sceglieremo sempre come rappresentante di una classe resto modulo n il suo unico numero b con $0 \le b \le n-1$.

Proviamo ad usare il prodotto per cifrare. Fissiamo un valore $\bar{a} \in \mathbf{Z}_{21}$ e proviamo a usare, come funzione cifrante, la sostituzione:

$$\mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\bar{m} \mapsto \bar{a} \cdot \bar{m}$$

Proviamo a vedere cosa succede moltiplicando per $\bar{3}$ e per $\bar{5}$:

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

Non bisogna pensare che tutte le proprietà con cui siamo soliti lavorare in $\mathbf{Z}$ restino valide in $\mathbf{Z}_n$. Ad esempio la legge di cancellazione $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{c} \Rightarrow \bar{b} = \bar{c}$ che vale in $\mathbf{Z}$ purché sia $a \neq 0$ non si trasporta alle congruenze; ad esempio:

$$3 \cdot 5 \equiv 3 \cdot 8 \equiv 6 \mod 9 \quad \text{ma non è vero che } 5 \equiv 8 \mod 9$$

Quindi non posso usare la moltiplicazione per $\bar{a}$ come funzione per cifrare, a meno che non scelga $\bar{a}$ con molta attenzione. **Quali sono i valori di $\bar{a}$ che vanno bene?**

TAVOLA 2.3 Cifrare con la moltiplicazione

Osserviamo rapidamente che se $n = p\,q$, allora le classi $\bar{p}$ e $\bar{q}$ non vanno bene: infatti,

$$\bar{p} \cdot \bar{q} = \bar{0} = \bar{p} \cdot \bar{0} = \bar{0} \cdot \bar{q}$$

Dunque la moltiplicazione per $\bar{p}$ e la moltiplicazione per $\bar{q}$ non definiscono una applicazione iniettiva in tal caso.

Possiamo dimostrare un risultato più generale:

Proposizione 1 *MCD(a,n) =1 se e solo se è biettiva la moltiplicazione*

(*)
$$\mathbf{Z}_n \to \mathbf{Z}_n$$
$$\bar{m} \mapsto \bar{a} \cdot \bar{m}$$

Dimostrazione Osserviamo che la moltiplicazione (*) è iniettiva se e solo se è biettiva. Dunque, basta controllare l'iniettività.
Supponiamo che *MCD(a,n) =1* e mostriamo che la moltiplicazione (*) è iniettiva.
Per ipotesi, n non divide a, e la classe $[a]$ è non nulla in $\mathbf{Z}_n$.
Prendiamo due numeri h e k con $h \neq k$ ed entrambi compresi tra 1 e *(n-1)*. Facciamo vedere che ak e ah non possono appartenere alla stessa classe di equivalenza, cioè che $(ak-ah) \neq tn$ per qualsiasi intero t. Infatti se fosse $ak - ah = t\,n$, allora sarebbe anche $a(k-h) = t\,n$; ma, poichè $MCD(a,n) =1$, n deve dividere $(h-k)$: ma questo è impossibile, perché $(h-k)$ è in valore assoluto minore di n.

Supponiamo ora che la moltiplicazione (*) sia iniettiva e mostriamo che $MCD(a,n) =1$.
Possiamo supporre che $0 < a < n$. Se, per assurdo, fosse $MCD(a,n) =d >0$, potremmo scrivere $n = d\,k$, $a = d\,h$ per opportuni interi $0 < h, k < n$. Ma allora, [0] ≠ [k] hanno la stessa immagine nella moltiplicazione (*): infatti

$$[k] \mapsto [a] * [k] = [ak] = [dh\,k] = [h\,n] = [0] = [a] * [0]$$

Abbiamo trovato un assurdo, quindi $MCD(a,n) =1$. ◊

Corollario *Se p è primo, è biettiva la moltiplicazione per ogni classe non nulla in* $\mathbf{Z}_p$.

Ora sappiamo come scegliere la classe $[a]$ in modo da ottenere una cifratura: ma come decifrare?

TAVOLA 2.4 e 2.5 'Decifrare' la moltiplicazione

Supponiamo che la moltiplicazione per $\bar{a}$ sia una applicazione iniettiva in $\mathbf{Z}_n$: poichè dominio e codominio hanno lo stesso numero finito di elementi, la moltiplicazione deve essere anche suriettiva, e **in particolare**

deve esistere $\bar{i}$ tale che $\bar{a} \cdot \bar{i} = \bar{1}$.

Definizione Una classe $\bar{a}$ in $\mathbf{Z}_n$ si dice **invertibile** se esiste $\bar{i}$ in $\mathbf{Z}_n$ tale che $\bar{a} \cdot \bar{i} = \bar{1}$. Una tale classe $\bar{i}$ è chiamata **inversa** di $\bar{a}$ in e talora si denota con il simbolo

$$\bar{a}^{-1}.$$

Ricordiamo che, in tal caso, $\bar{a} \cdot \bar{i} = \bar{i} \cdot \bar{a} = 1$.

Proposizione 2 *Una classe* $\bar{a}$ *è invertibile in* $\mathbf{Z}_n$ *se e solo se è biettiva la moltiplicazione*

$$(*) \qquad \begin{aligned} \mathbf{Z}_n &\to \mathbf{Z}_n \\ \bar{m} &\mapsto \bar{a} \cdot \bar{m} \end{aligned}$$

In tal caso, l'applicazione inversa di (*) è la moltiplicazione per l'inverso $\bar{a}^{-1}$ *di* $\bar{a}$*:*

$$(**) \qquad \begin{aligned} \mathbf{Z}_n &\to \mathbf{Z}_n \\ \bar{c} &\mapsto \bar{a}^{-1} \cdot \bar{c} \end{aligned}$$

Dimostrazione Abbiamo visto che l'invertibilità di $\bar{a}$ è una condizione necessaria affinchè la moltiplicazione sia biettiva.
Tale condizione risulta essere anche sufficiente. Basta provare che, se $\bar{a}$ è invertibile, allora (**) è la funzione inversa di (*), provando a comporre queste due funzioni.

$$\bar{m} \overset{(*)}{\mapsto} \bar{a} \cdot \bar{m} \overset{(**)}{\mapsto} \bar{a}^{-1} (\bar{a} \cdot \bar{m}) = \bar{a}^{-1} \cdot \bar{a} \cdot \bar{m} = \bar{m}$$

$$\bar{c} \overset{(**)}{\mapsto} \bar{a}^{-1} \cdot \bar{c} \overset{(*)}{\mapsto} \bar{a} \cdot (\bar{a}^{-1} \cdot \bar{c}) = (a \cdot \bar{a}^{-1}) \cdot \bar{c} = \bar{c}$$

Poichè entrambe le composizioni sono l'identità, la funzione (*) è invertibile, e (**) è la sua inversa. ◊

Come esercizio, dimostriamo direttamente che se $\bar{a}$ è invertibile, l'applicazione (*) è suriettiva; infatti, comunque scelto $\bar{q}$ in $\mathbf{Z}_n$, si può scrivere

$$\bar{q} = \bar{1} \cdot \bar{q} = (\bar{a} \cdot \bar{a}^{-1}) \cdot \bar{q} = \bar{a} \cdot (\bar{a}^{-1} \cdot \bar{q}) ;$$

dunque l'elemento $\bar{q}$ è immagine dell'elemento $\bar{m} = \bar{a}^{-1} \cdot \bar{q}$, *tramite l'applicazione (*)*: **ogni elemento del codominio appartiene all'immagine della moltiplicazione (*)**.

Se avessimo voluto provare in modo diretto l'iniettività di (*), potevamo procedere come segue: supponiamo che le classi $\bar{m}$ e $\bar{m}'$ abbiano la stessa immagine, cioè $\bar{a} \cdot \bar{m} = \bar{a} \cdot \bar{m}'$. Si ricava:

$$\bar{m} = \bar{1} \cdot \bar{m} = (\bar{a}^{-1} \cdot \bar{a}) \cdot \bar{m} = \bar{a}^{-1} \cdot (\bar{a} \cdot \bar{m}) = \bar{a}^{-1} \cdot (\bar{a} \cdot \bar{m}') = (\bar{a}^{-1} \cdot \bar{a}) \cdot \bar{m}' = \bar{1} \cdot \bar{m}' = \bar{m}' ,$$

da cui l'iniettività di (*).

Corollario 1 *Se $\bar{a}$ è invertibile, il suo inverso $(\bar{a})^{-1}$ è unico.*

Corollario 2 *La funzione (*) è una cifratura se e solo se $\bar{a}$ è invertibile. In tal caso, la funzione di decifratura è la moltiplicazione per l'inverso $\bar{a}^{-1}$.*

Corollario 3 *Una classe $\bar{a}$ in $\mathbf{Z}_n$ è invertibile se e solo se* MCD(a,n) = 1.

Corollario 4 *Se p è primo, ogni elemento non nullo $\bar{a}$ di $\mathbf{Z}_p$ è invertibile in $\mathbf{Z}_p \setminus \{\bar{0}\}$.*

A questo punto possiamo perfezionare la funzione di cifratura C_k usando la moltiplicazione. Possiamo definire un'applicazione C_k che contenga una moltiplicazione e una traslazione (così lo $\bar{0}$ non ha sè stesso come immagine). La nostra chiave sarà una coppia di numeri k = $(\bar{a}, \bar{b})$ e la funzione cifrante sarà

$$C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\bar{m} \mapsto \bar{a} \cdot \bar{m} + \bar{b}$$

Questo sistema prende il nome di **cifrario affine**.
La funzione C_k va bene se e solo se è biunivoca, cioè se e solo se è invertibile: si mostra facil;emte che ciò accade esattamente quando $\bar{a}$ invertibile. In tal caso, la funzione di decifratura è:

$$D_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\bar{c} \mapsto (\bar{a})^{-1} \cdot (\bar{c} - \bar{b})$$

Ad esempio, scegliamo $k = (\bar{5}, \bar{4})$, e consideriamo l'applicazione $C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$, definita da:

$$\bar{m} \mapsto \bar{5} \cdot \bar{m} + \bar{4}$$

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

La tabella visualizza i risultati ottenuti. Si vede che la funzione di chiave $k = (\bar{5}, \bar{4})$ è biunivoca, in quanto ad ogni lettera dell'alfabeto in chiaro resta associata una lettera diversa dell'alfabeto cifrato.

TAVOLA 2.6 A, B, C, D: distribuire una tavola, a scelta, e una copia dell'allegato per ciascuno dei ragazzi. Negli incontri successivi, i ragazzi completeranno la decifratura della frase nella tavola.
TAVOLA 2.7, 2.8 (facoltative)