Terza lezione

Ricordiamo alcuni risultati visti nella scorsa lezione: siamo abituati a utilizzare l'insieme dei numeri interi (o reali), che gode della seguente proprietà:

$$a \cdot m = 0 \text{ se e solo se o } a = 0 \text{ o } m = 0$$

Tale formula non è vera sempre in $\mathbf{Z}_n$. In $\mathbf{Z}_n$ la proprietà diventa:

$\bar{a} \cdot \bar{m} = \bar{0}$ se e solo se *$a \cdot m$ è un multiplo di n, cioè $a \cdot m = q \cdot n$ per un opportuno q*

Infatti, la classe di $a \cdot m$ modulo n è nulla se e solo $a \cdot m$ se è un multiplo di n. Abbiamo 2 possibili casi per cui il prodotto tra $\bar{a}$ e $\bar{m}$ risulti nullo:

1. $\bar{a} = \bar{0}$ oppure $\bar{p} = \bar{0}$ (cioè almeno uno tra a e m è multiplo di n)
2. $a \cdot m$ è un multiplo di n ma né a né m sono multipli di n. (ad esempio, $\bar{2} \cdot \bar{3} = \bar{0}$ modulo 6, ma né 2 né 3 sono multipli di 6)

Se n è un numero primo, il secondo caso non si può presentare.

Abbiamo introdotto la seguente definizione.

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

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

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

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

Cerchiamo dunque di caratterizzare le classi $\bar{a}$ invertibili (e di trovare esplicitamente l'inverso, quando esiste) .

Osserviamo subito che ogni classe $\bar{a}$ invertibile deve essere non nulla (cioè n non divide a) e a non può avere fattori in comune con n; dunque:

se $\bar{a}$ in $\mathbf{Z}_n$ è invertibile, allora MCD(a,n) = 1.

Questa è una condizione necessaria da imporre affinchè la moltiplicazione per $\bar{a}$ sia una cifratura in $\mathbf{Z}_n$.

Dimostreremo che vale il viceversa: se MCD(a,n) = 1, allora $\bar{a}$ è invertibile in $\mathbf{Z}_n$.

ALGORITMO EUCLIDEO e IDENTITA' DI BEZOUT

Ci proponiamo ora di fare una piccola digressione per introdurre una tecnica che sarà fondamentale per lo sviluppo del corso.

Sappiamo calcolare il MCD tra due numeri ragionevolmente piccoli (ad es. minori di 1000), di cui conosciamo (o possiamo facilmente calcolare) la scomposizione in fattori primi. Infatti, dati due numeri a,b e la loro scomposizione in primi, il MCD (a,b) si ottiene prendendo solo i fattori comuni con il minimo esponente.

L'algoritmo euclideo ci permette di poter calcolare il massimo comun divisore tra due numeri, anche se questi sono molto grandi, senza aver bisogno di fattorizzarli.
Ricordiamo, per completezza, alcune definizioni:

Definizione Dati due numeri interi a e b un loro **massimo comun divisore** è un intero positivo d, $d > 0$ tale che

1. d divide a e d divide b
2. se d' divide sia a che b allora d' divide d

Si dimostra, che ogni coppia di numeri interi a, b ammette un massimo comun divisore, che risulta essere unico, ed è indicato con il simbolo MCD(a,b).
Due numeri interi a, b tali che MCD(a,b) = 1 si dicono *coprimi* o *relativamente primi*.

Proposizione (divisione negli interi **Z**) Siano a, b numeri interi, con $b \neq 0$. Allora esistono e sono univocamente determinati due interi q e r tali che

$$a = b \cdot q + r \text{ con } 0 \leq r < |b|$$

In quest'operazione a è detto *dividendo*, b *divisore*, q *quoziente* e r *resto*
Dimostrazione. Sia $b \geq 0$, e tutti i suoi multipli sia positivi che negativi, e possiamo quindi avere la successione: $...,-kb...-2b,-b,0,b,2b,....kb....$ con $k>0$
Sicuramente esisteranno due multipli consecutivi di b tra cui è compreso a: $qb \leq a < (q+1)b$. Poniamo $r = a - qb$ e così abbiamo trovato i due numeri q e r richiesti. Osserviamo che tali numeri sono unici. Se b è un numero negativo, si avrà: $a = -b \cdot q' + r$ con $0 \leq r < |b| = -b$. Basta porre $q' = -q$. ◊

L'algoritmo euclideo, che consente di calcolare il M.C.D. tra due qualsiasi numeri, si basa su una serie di divisioni successive: si inizia dividendo a per b e si ottengono un quoziente q_1 e un resto r_1; se $r_1 = 0$, allora MCD(a,b)=b e ci si ferma; se $r_1 \neq 0$ si prosegue dividendo b per r_1 : si ottengono q_2 e r_2; se $r_2 = 0$, si interrompe il procedimento; se $r_2 \neq 0$, si itera il ragionamento. L'algoritmo termina quando troviamo resto nullo e il MCD è l'ultimo resto diverso da zero. Questa procedura ha sicuramente termine perché il resto si riduc ad ogni passo.
Il procedimento è illustrato di seguito, calcolando MCD(44880,5292).

$a = b * q + r$	a	=	b	*	quoziente	+	resto
44880= 5292*8+2544	44880	=	5292	*	8	+	2544
5292 = 2544 * 2 +204	5292	=	2544	*	2	+	204
2544 = 204 * 12 + 96	*2544*	=	204	*	12	+	96
204 = 96 * 2 + **12**	204	=	96	*	2	+	**12**
96 = 12 * 8 + 0 MCD	*96*	=	12	*	8	+	0

MCD (44880,5292) = 12 (=ultimo resto non nullo)

Piu in generale, dobbiamo calcolare MCD (a, b). Supponiamo $a \geq b > 0$ e operiamo le divisioni.

	a	=	**b**	*	**quoziente**	+	**resto**
$a = b * q_1 + r_1 \quad 0 < r_1 < b$	a	=	b	*	q_1	+	r_1
$b = r_1 * q_2 + r_2 \quad 0 < r_2 < r_1$	b	=	r_1	*	q_2	+	r_2
$r_1 = r_2 * q_3 + r_3 \quad 0 < r_3 < r_2$	r_1	=	r_2	*	q_3	+	r_3
…….					……		
$r_{i-2} = r_{i-1} * q_i + r_i \quad 0 < r_i < r_{i-1}$	$r_{i.\,-2}$	=	r_{i-1}	*	q_i	+	r_i
…….					……		
$r_{n-2} = r_{n-1} * q_n + r_n \quad 0 < r_n < r_{n-1}$	r_{n-2}	=	r_{n-1}	*	q_n	+	$\boldsymbol{r_n}$
$r_{n-1} = r_n * q_{n+1} + 0$	r_{n-1}	=	r_n	*	q_{n+1}	+	0

Allora MCD (a, b) = r_n (=ultimo resto non nullo).

Osservazioni.

1. L'ultimo resto non nullo r_n divide il resto precedente r_{n-1} , e dunque tutti i resti di indice più piccolo. Inoltre, r_n divide a e b. Dunque r_n divide il MCD che stiamo cercando.
2. Ogni divisore comune di a e b è anche divisore di r_1, perché se un numero divide a e b allora ne divide anche la differenza. Tale ragionamento vale per tutti i resti delle divisioni successive fino al resto r_n che è l'ultimo diverso da 0. Dunque ogni divisore comune di a e b deve dividere anche r_n.
3. Mettendo assieme le osservazioni 1 e 2 concludiamo che $r_n = MCD(a,b)$.
4. Al massimo occorre fare b operazioni, perché ogni resto r_i delle divisioni è minore del resto precedente, quindi abbiamo una catena $b>r_1>r_2>r_3>$.... di numeri che sono interi positivi e decrescenti, quindi hanno un minimo che è 0 e sono al massimo b.

TAVOLA 14:Calcolo del MCD

L'algoritmo di Euclide ci permette, una volta individuato d = MCD (a, b), di trovare due numeri interi s, t tali che

$$d = s * a + t * b$$

questa relazione si chiama **IDENTITA' DI BEZOUT**.

Per dimostrarla basta far vedere che tutti i resti delle divisioni successive si possono scrivere come combinazioni di a e b . Infatti osserviamo che, riscrivendo le divisioni operate, troviamo le relazioni:

$r_1 = a - b * q_1$
$r_2 = b - r_1 * q_2$
$r_3 = r_1 - r_2 * q_3$
……
$r_{n-1} = r_{n-3} - r_{n-2} * q_{n-1}$
$d = r_n = r_{n-2} - r_{n-1} * q_n$

Consideriamo l'ultima equazione, che descrive il massimo comun divisore d, che coincide con l'ultimo resto non nullo r_n, nei termini dei resti precedenti r_{n-2} e r_{n-1}. Sostituiamo il resto r_{n-1} con l'espressione $r_{n-1} = r_{n-3} - r_{n-2} * q_{n-1}$ ottenuta dalla penultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-2}.
Continuiamo sostituendo il resto r_{n-2} con l'espressione ottenuta dalla terzultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-4}. Si continua, utilizzando, in ordine inverso, tutte le equazioni.
Al termine, si ottiene una espressione di d = MCD(a,b) della forma cercata.

Notiamo che l'espressione del MCD (a, b) fornita dall'identità di Bezout non è affatto unica. Ad esempio: 1= 3*7+(–4)*5 .

Utilizzando l'esempio precedente, vediamo come procedere per trovare un'identità di Bezout. Dobbiamo individuare $s,t \in Z$ tali che 12 = s * 44880 + t * 5292. Riscriviamo i passaggi dell'algoritmo euclideo nel modo seguente:

44880 = 5292*8+2544 ⟶ r_1= 2544=44880 - 5292*8

5292 = 2544*2+204 ⟶ r_2 = 204 = 5292 - 2544*2

2544 = 204*12+96 ⟶ r_3 = 96 = 2544 - 204*12

204 = 96*2+12 ⟶ MCD =r_4= 12=204 - 96*2

Partiamo dall'ultima relazione scritta, sostituiamo il numero esplicitato nell'equazione precedente, raccogliamo i fattori comuni e continuiamo a sostituire fino ad ottenere un'espressione nei numeri a, b. Ovvero:

12 = 204 –96*2 = 204 – (2544 - 204*12)*2=
= 204 – 2544 *2 – 204*24
= 204 * 25 – 2544 *2 = (5292 - 2544*2) * 25 – 2544 *2
= 5292 * 25 – 2544 *52 = 5292* 25 –(44880-5292*8) *52
= 5292 * 441 – 44880 *52

$$12 = 441 * 5292 - 52 * 4480$$

Quindi abbiamo ottenuto 12 = (-52) * 44880 + 441 *5292, ovvero s = –52 e t = 441.

COME TROVARE L'INVERSO IN Z_n.

Siamo finalmente pronti ad applicare quanto abbiamo provato. Se MCD(a,n)=1, allora, in base alla relazione di Bezout, esistono interi s e t tali che

$$1 = s * a + t * n .$$

Prendendo le classi modulo n, scopriamo che

$$[1] = [s] * [a] + [t] * [n] = [s] * [a] + [t] * [0] = [s] * [a]$$

Dunque $[a]$ è invertibile, e $[s]$ è il suo inverso.

TAVOLA 15: L'identità di Bezout e l'inverso di un elemento

IL CIFRARIO DI VIGENÈRE

Introdotto da Blaise de Vigenère (1523-1596), segretario del Re di Francia, il cifrario di Vigenère è una generalizzazione del cifrario di Cesare poiché si realizza mediante una sequenza di sostituzioni monoalfabetiche applicate periodicamente. In questo sistema, ogni lettera in chiaro viene cifrata con un cifrario di Cesare la cui chiave dipende dalla posizione della lettera stessa. Per memorizzare come varia la chiave da utilizzare, si utilizza una tavola quadrata le cui righe contengono alfabeti ordinati traslati. Nella tavola usata negli esempi l'alfabeto è di 26 caratteri; la prima riga è riservata all'alfabeto in chiaro e la prima colonna alla lettura della chiave.

a b c d e f g h i l k l m n o p q r s t u v w x y z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H **I** J K L M N O P S
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

ISTRUZIONI PER CIFRARE.

I) Mittente e destinatario concordano la parola chiave, ad esempio LUCE.

II) La chiave deve essere ripetuta, carattere per carattere, sopra (o sotto) il messaggio in chiaro: ad ogni lettera del messaggio in chiaro, è così attribuita una lettera che dipende dalla sua posizione, da considerare come chiave.

Testo in chiaro APPUNTAMENTO AL MUSEO

L	U	C	E	L	U	C	E	L	U	C	E	L	U	C	E	L	U	C
A	P	P	U	N	T	A	M	E	N	T	O	A	L	M	U	S	E	O

III) ogni lettera del messaggio in chiaro (letta sulla prima riga della tabella) individua una colonna nella tabella. La lettera-chiave (letta sulla prima colonna della tabella) individua una riga della tabella.
Ogni lettera del messaggio in chiaro viene cifrata sostituendole la lettera nell'intersezione tra la colonna da essa individuata e la riga individuata dalla lettera-chiave. Nel nostro esempio A→ **L** e P→ **J**
IV) Si ripetono le operazioni per tutta la lunghezza del testo.
Testo cifrato LJRYYNCQPHVSLFOYDYQ

Si osservi che vengono utilizzate solo le righe coinvolte dalla parola chiave. Per semplificare il lavoro, è possibile metterle in evidenza. Si osservi, inoltre, che la lettera in chiaro A viene sempre cifrata con la lettera-chiave.

ISTRUZIONI PER DECIFRARE. Il destinatario deve utilizzare la tavola seguendo il metodo inverso. Esempio: Testo cifrato MMIHZOEFXRVXN, Chiave VENTO

M	M	I	H	Z	O	E	F	X	R	V	X	N
V	E	N	T	O	V	E	N	T	O	V	E	N

Per decifrare la prima lettera (M) occorre cercarla nella riga corrispondente alla lettera (V) della chiave e quindi risalire lungo la colonna fino ad incontrare la lettera in chiaro (R). Si ripete per le altre lettere, trovando il testo in chiaro: RIVOLTA SEDATA

E ADESSO RICORRIAMO ALLA MATEMATICA.
Per cifrare il testo si può far ricorso alla matematica modulare. Le 26 lettere dell'alfabeto vengono poste in corrispondenza con i numeri naturali da 0 a 25, ordinatamente. La cifratura si ottiene sommando il numero associato alla lettera in chiaro al numero corrispondente alla lettera-chiave (modulo 26).

Riprendiamo l'Esempio 1:

chiave	L	U	C	E	L	U	C	E	L	U	C	E	L	U	C	E	L	U	C
	11	20	2	4	11	20	2	4	11	20	2	4	11	20	2	4	11	20	2
chiaro	A	P	P	U	N	T	A	M	E	N	T	O	A	L	M	U	S	E	O
	0	15	15	20	13	19	0	12	4	13	19	14	0	11	12	20	18	4	14
somma	11	9	17	24	24	13	2	16	15	7	21	18	11	5	14	24	13	24	16
cifrato	L	J	R	Y	Y	N	C	Q	P	H	V	S	L	F	O	Y	N	Y	Q

A=0, L=11 A+L=0+11= 11 mod 26 e 11 → L
P=15, U=20 P+U=15+20=35 , 35 mod 26 =9 e 9 → J
e così si prosegue con le altre lettere ottenendo di nuovo il testo cifrato.
Per decrittare si procede allo stesso modo ma sottraendo anziché sommare.