Alcune applicazioni alla crittografia
Laboratorio di matematica – Scienze e tecnologie per i media – aa 2016-2017

Analizzeremo alcuni metodi di cifratura utilizzati nel corso della storia, prestando particolare attenzione all'impianto matematico che ne consente la realizzazione.

Sistema crittografico di Cesare
Il primo esempio è stato tramandato da Svetonio, uno storico del II sec d.C. Nella sua Vita dei Cesari parla di un sistema utilizzato da Cesare per cifrare i suoi messaggi: egli spostava di tre lettere ogni lettera del messaggio da inviare.
Se indichiamo con lettere minuscole le 21 lettere dell'alfabeto, ciascuna lettera del nostro messaggio (**testo in chiaro**) sarà sostituita con la lettera che si trova tre posizioni più avanti, e che per comodità indicheremo con caratteri maiuscoli, ottenendo così un nuovo messaggio (**testo cifrato**) apparentemente privo di significato

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

Ad esempio se il messaggio da inviare è il seguente:
La madre di Lancillotto era la sacerdotessa di Avalon
il risultato dopo la cifratura sarà:
OD PDGUH GN ODQFNOORZZR HUD OD VDFHUGRZHVVD GN DBDORQ

Possiamo decidere di generalizzare questo sistema decidendo di spostare le lettere non di tre posizioni ma di una quantità arbitraria:

Definizione Un sistema di questo tipo, in cui ogni lettera del testo cifrato è ottenuta da una lettera de testo in chiaro spostando di un certo numero di posizioni le lettere, prende il nome di **cifrario di Cesare** o di **cifratura per traslazione**.

Il numero di posizioni di cui spostare le lettere è una informazione aggiuntiva che permette di realizzare concretamente il metodo: essa viene detta **chiave di cifratura (o chiave cifrante)**.
Come si decifra? La chiave per decifrare si ricava in modo immediato dalla chiave per cifrare: basta spostarsi della stessa quantità di posizioni, ma nella direzione opposta.

Esercizio 1 Prepara l'alfabeto cifrante (in lettere maiuscole), spostando di 7 lettere aiutandoti con la griglia. Il numero 7 è la chiave cifrante.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

Cifra il seguente messaggio, utilizzando l'alfabeto preparato.

v	i	e	n	i		a	l		m	a	r	e	?						

Esercizio 2 A partire dalla chiave cifrante, ricava la chiave per decifrare. Decifra il messaggio, aiutandoti con la griglia dell'alfabeto. Il numero 9 è la chiave cifrante.
La chiave per decifrare è ……

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z

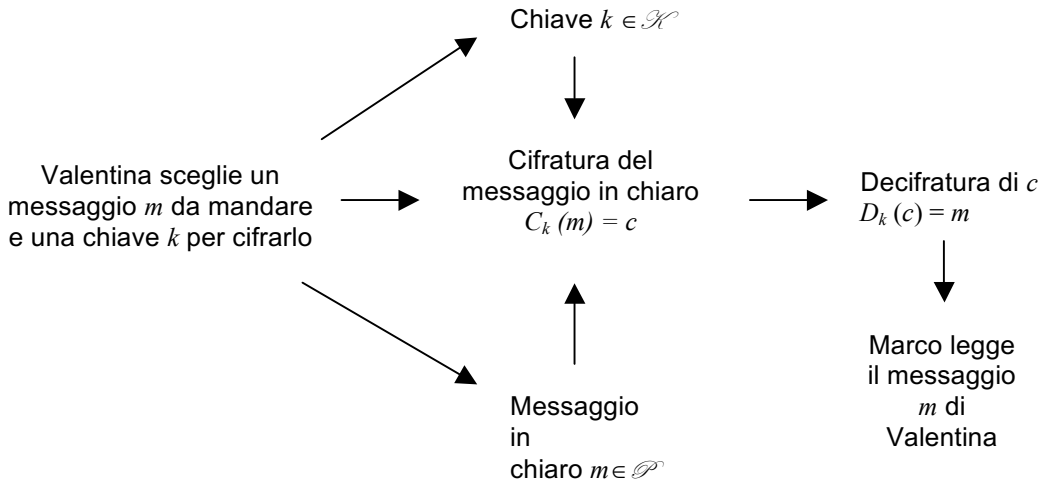
O	A	V	L	Z	T		B	T	A	H	P								

Sistemi crittografici
Discutiamo più in generale la nozione di crittografia.
La **cifratura** è una operazione di passaggio da un messaggio (detto **messaggio in chiaro**) ad un messaggio il cui significato è "nascosto" (detto **messaggio cifrato**): ad esempio il passaggio da un linguaggio ad un altro poco diffuso.

La cifratura permette quindi di passare dall'insieme dei messaggi in chiaro all'insieme dei messaggi cifrati: può dunque essere interpretata come una funzione tra questi due insiemi.
Possiamo cifrare singole parole (basta pensare ad un vocabolario inglese-italiano, ad esempio) o cifrare le singole lettere dell'alfabeto (come fa il cifrario di Cesare).

Un **crittosistema** è costituito da:
- l'insieme dei messaggi in chiaro $\mathscr{P}$ i cui elementi vengono indicati spesso con la lettera m;
- l'insieme delle chiavi $\mathscr{K}$ in cui ogni elemento k determina una trasformazione di cifratura C_k e una trasformazione di decifratura D_k che sono una l'inversa dell'altra;
- l'insieme dei messaggi cifrati $\mathscr{C}$ i cui elementi sono indicati spesso con la lettera c.

Un crittosistema è determinato da una terna $(\mathscr{P}, \mathscr{K}, \mathscr{C})$ e la comunicazione tra due persone, Valentina e Marco, può essere riassunta dal seguente diagramma:



Nel cifrario di Cesare:
- gli elementi $m \in \mathscr{P}$ sono le parole che vogliamo inviare (in una lingua fissata);
- la chiave consiste in fase di cifratura nello spostare di tre posti le varie lettere (C_k) e in fase di decifratura nel rimetterle nella loro corretta posizione (D_k);
- gli elementi c sono il risultato dell'operazione di cifratura.

Quali funzioni possono essere usate per cifrare?
Iniziamo considerando il caso in cui la trasformazione di cifratura opera sulle singole lettere dell'alfabeto: la cifratura può essere realizzata tramite una funzione tra l'alfabeto di partenza (detto **alfabeto in chiaro**) all'alfabeto d'arrivo (detto **alfabeto cifrante**): abbiamo bisogno che a lettere diverse dell'alfabeto in chiaro corrispondano

lettere diverse dell'alfabeto cifrante (perché questo ci assicura che, così, è possibile decifrare in modo univoco il testo).
La funzione cifrante deve quindi essere iniettiva, cioè ad elementi distinti dell'alfabeto in chiaro devono corrispondere elementi distinti dell'alfabeto cifrante. Ricordiamo che una funzione tra due insiemi A (dominio) e B (codominio) è biunivoca se è iniettiva e suriettiva. È iniettiva se ad elementi distinti di A corrispondono elementi distinti di B. È suriettiva se ogni elemento di B è immagine di almeno un elemento di A.
Chi riceve un messaggio cifrato deve essere in grado di interpretarlo ("decifrare").
Valentina e Marco si devono essere messi d'accordo prima su come "cifrare" e "decifrare" e scegliere un metodo efficace in modo che per gli altri sia sostanzialmente impossibile cifrare e decifrare un messaggio

Ci occuperemo soprattutto dei sistemi di cifratura che operano sulle singole lettere dell'alfabeto.
Per semplicità, supponiamo che l'alfabeto cifrante contenga solo lettere che si ottengono cifrando le lettere dell'alfabeto in chiaro; non introduciamo elementi di disturbo nell'alfabeto cifrante.
Nel nostro caso, quindi, **dobbiamo verificare che la funzione cifrante C_k sia biunivoca**:

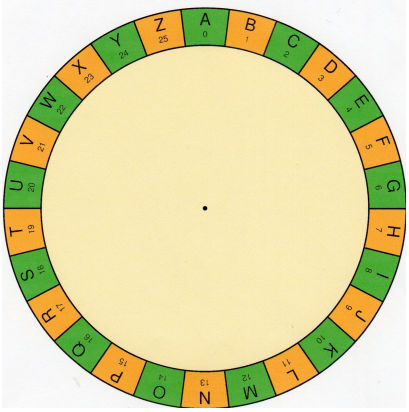
- prese due lettere distinte dell'alfabeto in chiaro queste vengano criptate con lettere diverse (iniettività)
- ogni lettera dell'alfabeto cifrante è la cifratura di (almeno) una lettera dell'alfabeto in chiaro (suriettività).

Anche se una funzione C_k è biunivoca, può non risultare opportuna dal punto di vista crittografico: ad esempio, la funzione che associa ogni lettera a se stessa (l'identità) produce un testo cifrato identico a quello in chiaro, e non è vantaggiosa. Più in generale, si chiederà che la funzione di cifratura non cifri mai una lettera con se stessa: dopo aver controllato la biettività della funzione cifrante, occorrerà discutere separatamente la sua convenienza da un punto di vista crittografico.
Le possibilità per i cifrari di Cesare nel caso della lingua italiana sono solamente 20 perché ovviamente se una lettera si sposta di 21 posizioni, ritorna al punto di partenza. Mentre nel caso dell'alfabeto inglese abbiamo 25 alfabeti cifranti possibili dato che le lettere sono 26.

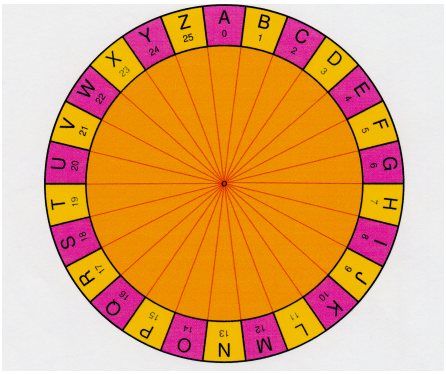
NOMENCLATURA:
Cifratura: passaggio da un messaggio (detto messaggio in chiaro) ad un messaggio (detto messaggio cifrato) il cui significato è nascosto. Questo passaggio è svolto attraverso una funzione cifrante
Decifratura: operazione di recupero del significato originale (messaggio in chiaro) a partire dal messaggio cifrato.
Alfabeto in chiaro: alfabeto che permette di scrivere tutti i messaggi richiesti
Alfabeto cifrante: alfabeto che permette di scrivere tutti i messaggi richiesti, ma il cui significato non è immediatamente chiaro.
Chiave di cifratura: informazione aggiuntiva che permette di applicare concretamente la cifratura
Chiave di decifratura: informazione aggiuntiva che permette di applicare concretamente la decifratura

Le classi resto modulo n

Abbiamo visto che volendo cifrare un messaggio usando il metodo di Cesare dobbiamo sostanzialmente traslare le lettere di una certa quantità di posizioni (che decidiamo noi e rappresenta la chiave utilizzata per cifrare). Tale operazione diventa più rapida utilizzando un cifrario rotondo. Proviamo a rappresentare il metodo, utilizzando l'alfabetico.



L'alfabeto in chiaro



L'alfabeto cifrante (su un cerchio più piccolo)

Sovrappongo i due cerchi e faccio ruotare l'alfabeto cifrante in base alla chiave di Cesare fissata.

Possiamo interpretare così la procedura seguita: assegniamo ad ogni lettera dell'alfabeto italiano in chiaro un numero corrispondente alla sua posizione come nella seguente tabella:

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

Tabella 1

Dopodichè decidiamo un numero (ad esempio 5) che rappresenta la nostra chiave e lo sommiamo ad ogni posizione così da ottenere che nell'alfabeto cifrante la A corrisponda alla lettera in posizione 5 cioè alla F, la B alla G,…, la R alla Z, la S che occupa la posizione 16 corrisponda alla A, la T alla B,…., la Z alla E.
Il nodo fondamentale di questa procedura sta nel fatto che quando abbiamo deciso la corrispondenza tra la T e la B abbiamo sostanzialmente ragionato così:

- la lettera T occupa la posizione 17 (ricorda che partiamo dalla posizione 0),
- 17+5=22 ma le posizioni possibili sono 21 e sono numerate da 0 a 20 quindi il numero 22 non corrisponderebbe a nessuna lettera
- $22 = 1 \cdot 21 + 1$ e abbiamo deciso che la lettera T doveva corrispondere a quella in posizione 1 cioè alla B

Ed è per questo motivo che la lettera S corrisponde alla A (perché S= posizione 16, 16+5=21, $21 = 1 \cdot 21 + 0$ e la lettera A occupa la posizione 0), la U alla C e così via.
Quindi da un punto di vista matematico quando cifriamo con questo metodo operiamo una somma (per traslare) dopodichè se il risultato è maggiore di *21* ci interessiamo solo al resto della divisione per *21*: le lettere dell'alfabeto sono in corrispondenza biunivoca con i possibili resti della divisione di un intero per *21*. Ogni numero intero rappresenta una lettera: per sapere quale, basta calcolare il suo resto nella divisione per *21* e usare la Tabella 1 per individuare la lettera corrispondente.

(attento alle divisioni in cui compaiono numeri negativi: il resto è l'unico c compreso tra 0 e 20 tale $a = 21 \cdot q + c$ per un numero intero q.)

Proviamo a generalizzare, lasciando libero il numero delle lettere dell'alfabeto, che denoteremo con n *(*con n maggiore di 0*)*: in un alfabeto di n lettere, possiamo chiamare 0, 1, ..., $n-1$ le lettere e **identificare due numeri che abbiano lo stesso resto nella divisione per *n***. Per brevità, diciamo che due numeri che hanno lo stesso resto nella divisione per n sono **congruenti modulo *n* (o mod *n*)** e introduciamo un simbolo: se due numeri $a, b \in \boldsymbol{Z}$ sono ***congruenti modulo n***, scriviamo

$$a \equiv b \bmod n$$

Talora, usiamo l'aggettivo 'congruo' al posto di 'congruente'.
Osserviamo, per definizione, che **ogni numero *a* è congruente mod *n* al suo resto nella divisione per *n*, cioè all'unico *c* compreso tra *0* e *n–1* tale che $a = n \cdot q + c$ per un intero *q*.** Dunque, un qualsiasi numero intero (positivo o negativo) è congruente modulo n ad uno e ad uno solo tra i numeri 0, … , $n–1$.

Cerchiamo di riformulare questo concetto, per poter verificare in modo diretto se due numeri sono congruenti modulo n, senza bisogno di calcolare esplicitamente i resti della divisione per n. Si verifica facilmente che:

Definizione Sia n un intero positivo fissato. Due numeri $a, b \in \boldsymbol{Z}$ sono ***congruenti modulo n*** se e solo se $a–b$ è un multiplo di n, ovvero,

$$a \equiv b \bmod n \Leftrightarrow (a–b) = n \cdot h \text{ per qualche } h \in \boldsymbol{Z}.$$

Esempi:

1. $25 \equiv 1 \bmod 3$ perché $25 – 1 = 24 = 3 \cdot 8$.
2. $67 \equiv 55 \bmod 6$ perché $67 – 55 = 12 = 6 \cdot 2$.
3. $55 \equiv 1 \bmod 6$ perché $55 – 1 = 54 = 6 \cdot 9$.
4. $–5 \equiv 1 \bmod 6$ perché $–5 – 1 = –6 = 6 \cdot (–1)$.

Osservazioni. Chiamiamo 'congruenza' la relazione definita sugli interi dall'essere congruenti.

1. Ogni numero è congruente a sè stesso, modulo qualsiasi n: dunque per la congruenza vale la *proprietà riflessiva*.
2. $a \equiv b \bmod n \Leftrightarrow (a – b) = n \cdot h \Leftrightarrow (b – a) = n \cdot (-h) \Leftrightarrow b \equiv a$: dunque per la congruenza vale la *proprietà simmetrica*.
3. Notiamo che gli esempi 2 e 3 ci suggeriscono la transitività della congruenza. Infatti vale anche che $67 \equiv 1 \pmod 6$ perché $67 – 1 = 66 = 6 \cdot \mathbf{11}$.
   Più in generale se , $a \equiv b \bmod n$, cioè $(a–b) = n \cdot h$ e $b \equiv c \bmod n$, cioè $(b–c) = n \cdot k$, allora
   $(a–c) = (a – b + b – c) = (a – b) + (b – c) = n \cdot h + n \cdot k = n \cdot (h+k)$ e dunque $a \equiv c \bmod n$. Dunque per la congruenza vale la *proprietà transitiva*.
4. **La congruenza modulo *n* è una relazione di equivalenza.**

La congruenza divide quindi gli interi in sottoinsiemi tra loro disgiunti:
Definizione Dato $a \in \boldsymbol{Z}$, si denota con $\overline{a}$ l'insieme

$$\overline{a} = \{ b \in \boldsymbol{Z} \text{ tale che } b \equiv a \bmod n\} \text{ detto } \textbf{\textit{classe resto modulo n}}$$

e si dice che a **rappresenta** (o **è rappresentante di**) tale insieme.

Diciamo anche che $\overline{a}$ è *a* modulo *21* (in simboli*: a mod 21*). Useremo anche il simbolo *[a]* per denotare la classe resto rappresentata da *a* mod *n*. A partire dalla prossima lezione, quando sarà chiara la distinzione tra il numero *a* e la sua classe, scriveremo semplicemente *a* per denotare il numero o la sua classe.
Come già osservato, fissato *n*, un qualsiasi numero intero (positivo o negativo) è congruo modulo *n* ad uno e ad uno solo tra i numeri 0, … , *n–1*. Dunque le classi resto modulo *n* sono esattamente *n* e ciascuna di esse ha uno ed un solo rappresentante in

$$\{ 0, 1, 2, ..., n–1 \} .$$

Cercheremo di usare sempre il rappresentante della classe scelto con questo criterio.
ESEMPIO Possiamo calcolare tutte le classi resto modulo 4:
$\overline{0}$ = { …….., -16, -12, -8, -4, 0, 4, 8, 12, ….}= interi che divisi per 4 danno resto 0
$\overline{1}$ = { …….., -15, -11, -7, -3, 1, 5, 9, 13, ….}= interi che divisi per 4 danno resto 1
$\overline{2}$ = { …….., -14, -10, -6, -2, 2, 6, 10, 14, ….}= interi che divisi per 4 danno resto 2
$\overline{3}$ = { …….., -13, -9, -5, -1, 3, 7, 11, 15, ….}= interi che divisi per 4 danno resto 3

Riprendiamo il cifrario di Cesare. Possiamo dire che usiamo come lettere dell'alfabeto in chiaro i numeri interi compresi tra 0 e 20 e che, per criptare tramite un cifrario di Cesare, lavoriamo modulo 21; ad esempio, usiamo come chiave $k = 71$ (cioè trasliamo di 71 posizioni) e cifriamo la lettera D, che corrisponde al numero 3: per cifrarla, devo calcolare 3+71 = 74. Per capire esattamente la posizione di 74 modulo 21 nel mio orologio con 21 ore, devo determinare il numero *c* compreso tra 0 e 20 che sia congruo a 74 modulo 21. Verifico che $74 = 3 \cdot 21 + 11 \equiv 11 \bmod 21$, e cifro la lettera D con 11.
Come lettere dell'alfabeto (in chiaro e cifrante) non uso più i numeri 0, … , *n–1*, ma le classi da essi rappresentate modulo 21:

Definizione L'insieme delle classi resto modulo *n* si indica con $\mathbf{Z}_n = \{ \overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1} \}$

Di solito, sceglieremo come rappresentante di una classe resto modulo *n* il suo unico numero *b* con

$$0 \le b \le n–1$$

Proprio come in **Z**, si possono definire operazioni che ci consentono di trattare le classi resto come numeri. Iniziamo definendo la somma.

Definizione In $\mathbf{Z}_n$ si definisce la somma di due classi resto $\overline{a}$ e $\overline{b}$ modulo *n* nel modo seguente: $\overline{a} + \overline{b} = \overline{a+b}$

Ricordando la Tabella 1 dell'associazione lettera-numero, l'alfabeto numerico dei messaggi unitari (le singole lettere) è quindi rappresentato da $\mathscr{P} = \mathbf{Z}_{21}$.
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 $\mathscr{K} = \{ 0, 1, 2, ..., 20\}$.
Il sistema crittografico per traslazione può essere così schematizzato:
data la chiave $k \in \mathscr{K}$, la funzione cifrante sarà la seguente:

$$C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\overline{m} \to \overline{m+k} \bmod 21,$$

mentre la funzione inversa, quella di decifratura, sarà:

$$D_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\overline{c} \to \overline{c-k} \mod 21.$$

Sapendo che un testo è stato cifrato con il metodo di Cesare, è possibile recuperarne il testo in chiaro procedendo per tentativi, cioè provando tutte le 20 chiavi possibili. Occorre dunque cercare un metodo di cifratura più efficace e sicuro.

Esercizio Per ogni classe resto modulo *n*, elenca alcuni elementi che appartengono alla classe e determina il rappresentante compreso tra 0 e *n*-1, come nell'esempio:

12 modulo 5 : {2,7,12,17,-3,-8....}

12 modulo 4 : .....

– 1 modulo 6 : .....

74 modulo 23 : .....

–7 modulo 5 : .....

–13 modulo 12 : .....

63 modulo 7 : .....

Esercizio Stabilisci se le seguenti congruenze sono verificate:

16≡31 mod 5	V□ F□
25≡13 mod 13	V□ F□
72≡-21 mod 31	V□ F□
82≡59 mod 29	V□ F□
27255≡79081 mod 79	V□ F□
28157≡-1517 mod 37	V□ F□

Esercizio Completa le tavole con le somme modulo 5

+	0	1	2	3	4
0					
1					
2					
3					
4					

modulo 6

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Esercizio Decifra il seguente messaggio numerico sapendo che è stato utilizzato il sistema di cifratura:

$$C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\overline{m} \to \overline{m+14} \mod 21.$$ **Messaggio cifrato: 16 1 9 18 8 12 5 4 5 4 11 5 12 18 14 8 3 14 10 11 8 18**

Tabella di conversione dell'alfabeto in chiaro

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

Determina la funzione di decifratura e aiutati con questa tabella, calcolando la funzione di decifratura e poi convertendo i numeri ottenuti nell'alfabeto in chiaro

16	1	9	18	8	12	5	4	5	4	11	5	12	18	14	8	3	14	10	11	8	18

Il prodotto nelle classi resto

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. Oltre alla somma, è possibile definire il prodotto e creare tutta un'aritmetica che viene definita *aritmetica modulare* perché si lavora modulo n.

Definizione 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 $a \equiv a'$ mod n e $b \equiv b'$ mod 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 $a+b \equiv a'+b'$ mod 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 $a \cdot b \equiv a' \cdot b'$ mod n e il prodotto è ben definito.
Ad esempio: [18]+[21] = [3] mod 4 : infatti 18+21 = 39 e [39] = [3] mod 4 perché $39 = 4 \cdot 9 + 3$.
D'altronde, [18] = [2] (perché $18 = 4 \cdot 4 + 2$) e [21] = [1] perché $21 = 4 \cdot 5 + 1$: 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.

Esercizio Completare le tavole dei prodotti

Modulo 5

×	0	1	2	3	4
0					
1					
2					
3					
4					

×	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Modulo 6

Modulo 9

×	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

Applicazioni del prodotto alla crittografia

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 **Z** : infatti, preso un qualsiasi elemento $\bar{a} \in \mathbf{Z}_n$ vale che:

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

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:

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

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
5m	**0**	**5**	**10**	**15**	**20**	**4**	**9**	**14**	**19**	**3**	**8**	**13**	**18**	**2**	**7**	**12**	**17**	**1**	**6**	**11**	**16**
3m	**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 **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 **Z** purché sia $a \neq 0$ non si trasporta alle congruenze; ad esempio:

$3 \cdot 5 \equiv 3 \cdot 8 \equiv 6 \bmod 9$ ma non è vero che $5 \equiv 8 \bmod 9$

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?**

Esercizio Cifrare con la moltiplicazione

1.Osserva con attenzione la tabella della moltiplicazione **modulo 5.**
Costruisci la funzione che si ottiene moltiplicando ogni elemento per **3**, cioè congiungi con una freccia l'elemento $\bar{a}$ della prima colonna con l'elemento $f(\bar{a}) = 3 \cdot \bar{a}$ della seconda colonna.

	× 3	
0		0
1		1
2		2
3		3
4		4

E' una funzione adatta per crittografare? E' iniettiva? E' suriettiva?

2. Osserva con attenzione la tabella della moltiplicazione **modulo 6.** Costruisci la funzione che si ottiene moltiplicando ogni elemento per **3**, cioè congiungi con una freccia l'elemento $\bar{a}$ della prima colonna con l'elemento $f(\bar{a}) = 3 \cdot \bar{a}$ della seconda colonna.

	× 3	
0		0
1		1
2		2
3		3
4		4
5		5

E' una funzione adatta per crittografare? E' iniettiva? E' suriettiva?

3. Modulo 6, costruisci ora la funzione che si ottiene moltiplicando ogni elemento per **5**, cioè congiungi con una freccia l'elemento $\bar{a}$ della prima colonna con l'elemento $g(\bar{a}) = 5 \cdot \bar{a}$ della seconda colonna.

	× 5	
0		0
1		1
2		2
3		3
4		4
5		5

4. Descrivi e studia in modo analogo la moltiplicazione per 4 modulo 9.

Osserviamo rapidamente che se $n = p\,q$, allora le classi $\bar{p}$ e $\bar{q}$ non vanno bene come fattori per ottenere una funzione cifrante: 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 *La moltiplicazione*

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

è biettiva se e solo se MCD(a,n) =1.

Dimostrazione 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 $\bar{a}$ 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, $\bar{0} \neq \bar{k}$ hanno la stessa immagine nella moltiplicazione (*): infatti

$$\bar{k} \to \bar{a} \cdot \bar{k} = \bar{ak} = \bar{dhk} = \bar{hn} = \bar{0} = \bar{a} \cdot \bar{0}$$

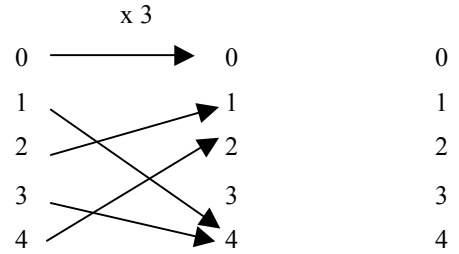
Abbiamo trovato un assurdo (perché la moltiplicazione non sarebbe iniettiva), quindi *MCD(a,n) =1.* ◊

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

Classi resto invertibili

Ora sappiamo come scegliere la classe $\bar{a}$ in modo che la moltiplicazione per $\bar{a}$ sia una funzione cifrante: ma come decifrare?

1. **Esercizio** Abbiamo visto che **la moltiplicazione per 3, modulo 5,** è iniettiva. Costruisci con le frecce la corrispondente funzione inversa:



2. Controlla se la funzione inversa coincide con la moltiplicazione, modulo 5, per uno di questi numeri: 2, 3, 4.

x 2	
0	0
1	1
2	2
3	3
4	4

x 4	
0	0
1	1
2	2
3	3
4	4

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

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

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

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

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.

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

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

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

Corollario

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

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

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

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

Cifrario affine

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 se stesso come immagine). La nostra chiave sarà una coppia di classi resto $k = (\bar{a}, \bar{b})$ e la funzione cifrante sarà

$$\begin{aligned} C_k : \mathbf{Z}_{21} &\to \mathbf{Z}_{21} \\ \bar{m} &\to \bar{a} \cdot \bar{m} + \bar{b} \end{aligned}$$

Questo sistema prende il nome di **cifrario affine**.

Come abbiamo visto, la funzione C_k va bene se e solo se $\bar{a}$ invertibile. In tal caso, la funzione di decifratura è:

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

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

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

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.

C_k	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**

Per decifrare, occorre calcolare $\bar{c} \to (\bar{a})^{-1} \cdot (\bar{c} - \bar{b})$, cioè

$$\bar{c} \to (\bar{5})^{-1} \cdot (\bar{c} - \bar{4}) = (\bar{5})^{-1} \cdot (\bar{c} + \bar{17}) \text{ (ricordando che } -\bar{4} = \bar{17})$$

Ma quale è la classe resto $(\bar{5})^{-1}$ in $\mathbf{Z}_{21}$? Poiché $(-\bar{4}) \cdot \bar{5} = -\bar{20} = \bar{1}$, scopriamo che

$$-\bar{4} = \bar{17} = (\bar{5})^{-1} .$$

La funzione per decifrare è dunque

$$D_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21},$$
$$\bar{c} \to \bar{17} \cdot (\bar{c} + \bar{17}) = \bar{17} \cdot c + \bar{16}$$

D_k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
17 c+16	16	12	8	4	0	17	13	9	5	1	18	14	10	6	2	19	15	11	7	3	20

In generale, per poter decifrare, devo riuscire a calcolare in modo esplicito $(\bar{a})^{-1}$. Per imparare a farlo, dobbiamo studiare meglio le classi resto.

MASSIMO COMUNE DIVISORE E ALGORITMO DI EUCLIDE

L'algoritmo di Euclide permette di calcolare il massimo comun divisore tra due numeri, anche se questi sono molto grandi, senza aver bisogno di fattorizzarli come prodotto di fattori primi.
Ricordiamo, per completezza, alcune definizioni:

Definizione Siano dati due numeri naturali non nulli *a* e *b*. Un loro **massimo comun divisore** è un numero naturale non nullo *d*, tale che

1. *d* divide *a* e *d* divide *b* (cioè *d* è un divisore comune)
2. *d* è il numero più grande con tale proprietà.

Se *a* e *b* non sono entrambi nulli, l'insieme dei loro divisori comuni è non vuoto (contenendo almeno 1) e finito (perchè i divisori di un numero non nullo non possono essere maggiori del numero stesso). Poichè i numeri naturali formano un insieme ordinato, il massimo comune divisore esiste sempre, ed è unico: esso viene indicato con il simbolo MCD(*a,b*).

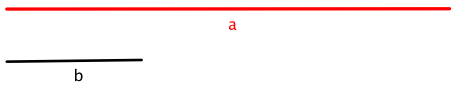
Due numeri naturali non nulli *a, b* tali che MCD(*a,b*) = *1* si dicono *coprimi* o *relativamente primi*.

La divisione tra numeri naturali può essere riletta nel modo seguente:
Proposizione Siano *a*, *b* numeri naturali non nulli. Allora esistono e sono univocamente determinati due interi *q* e *r* tali che

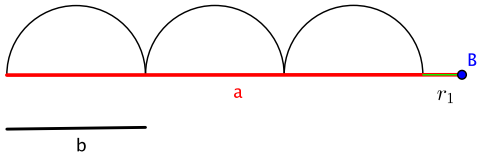
$a = b \cdot q + r$ con $0 \le r < b$

In quest'operazione *a* è detto *dividendo*, *b divisore*, *q quoziente* e *r resto.*

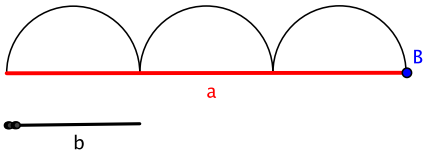
L'**algoritmo di Euclide** (o **metodo delle divisioni successive**), che consente di calcolare il MCD tra due qualsiasi numeri, si basa su una serie di divisioni successive:



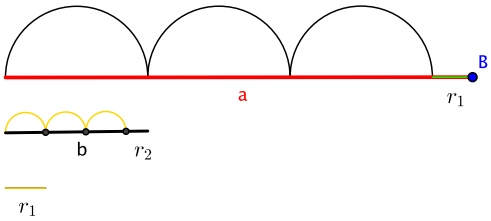
si inizia dividendo a per b e si ottengono un quoziente q_1 e un resto r_1;



se $r_1 = 0$, allora b divide a



quindi 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 ripete il ragionamento:
- disegno un nuovo segmento, r_2
- divido il segmento precedente r_1 per r_2, ottenendo q_3 e r_3 tali che

$$r_1 = r_2 \cdot q_3 + r_3 \, .$$

- se $r_3 = 0$, allora r_2 divide r_1 . Ma allora r_2 divide anche $b = r_1 \cdot q_2 + r_2$. Concludiamo che r_2 divide $a = b \cdot q_1 + r_1$. Dunque, r_2 è un divisore comune di a e b. Ma qualsiasi divisore comune di a e b deve dividere $r_1 = a - b \cdot q_1$ e quindi anche $r_2 = b - r_1 \cdot q_2$. Concludiamo che

$$r_2 = \text{MCD}(a,b)$$

Osserviamo che il MCD r_2 è l'ultimo resto non nullo e che abbiamo ottenuto la risposta cercata.
Se, invece, $r_3 \neq 0$, si aggiunge un nuovo segmento e si ripete il ragionamento precedente. **L'algoritmo termina quando troviamo resto nullo e il MCD è l'ultimo resto diverso da zero**. La procedura ha sicuramente termine perché il resto si riduce ad ogni passo.

Il procedimento è illustrato di seguito, calcolando MCD (44880,5292).
$a = b \cdot q + r$

44880 = 5292 · 8+2544

5292 = 2544 · 2 +204

2544 = 204 · 12 + 96

204 = 96 · 2 + **12**

96 = 12 · 8 + 0 ← MCD

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

Esempio

1) Calcola MCD (1637,31)

44880 = 31 · 52 + 25

31 = 25 · 1 + 6

25 = 6 · 4 + **1**

6 = 1 · 6 + **0** ← MCD

MCD (1637,31) = 1 (=ultimo resto non nullo)

2) Calcola MCD (1763,51)

1763 = 51 · 34 + 29

51 = 29 · 1 + 22

29 = 22 · 1 + 7

22 = 7 · 3 + **1**

7 = 1 · 7 + 0 ← MCD

MCD (1763,51)= 1 (=ultimo resto non nullo)

3) Calcola MCD (1547, 560)

1547 = 560 · 2 + 427

560 = 427 · 1 + 133

427 = 133 · 3 + 28

133 = 28 · 4 + 21

28 = 21 · 1 + 7 ← MCD

21 = 7 · 1 + 0

MCD (1547,560)= 7 (=ultimo resto non nullo)

Esercizi Calcola, con il metodo di Euclide, i seguenti numeri:
MCD(2337, 1482)= …..
MCD(16717, 8249)= …..
MCD(4891, 1541)= …..

Identità di Bézout

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

$$d = s \cdot a + t \cdot b$$

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

Vediamo il procedimento per trovare un'identità di Bezout in un esempio, riprendendo i calcoli fatti per calcolare MCD (44880,5292) = 12.

Dobbiamo individuare $s, t \in \mathbf{Z}$ tali che $12 = s \cdot 44880 + t \cdot 5292$. Riscriviamo i passaggi dell'algoritmo euclideo nel modo seguente:

$44880 = 5292 \cdot 8 + 2544 \longrightarrow r_1 = 2544 = 44880 - 5292 \cdot 8$

$5292 = 2544 \cdot 2 + 204 \longrightarrow r_2 = 204 = 5292 - 2544 \cdot 2$

$2544 = 204 \cdot 12 + 96 \longrightarrow r_3 = 96 = 2544 - 204 \cdot 12$

$204 = 96 \cdot 2 + 12 \longrightarrow \text{MCD} = r_4 = 12 = 204 - 96 \cdot 2$

Partiamo dall'ultima relazione scritta e sostituiamo in essa il numero esplicitato nell'equazione subito precedente; raccogliamo i fattori comuni e continuiamo a sostituire il resto dell'equazione precedente (procedendo dal basso verso l'alto) fino ad ottenere un'espressione nei numeri a, b. Otteniamo:

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

$$\boxed{12 = 441 \cdot 5292 - 52 \cdot 4480}$$

Quindi abbiamo ottenuto $12 = (-52) \cdot 44880 + 441 \cdot 5292$, ovvero $s = -52$ e $t = 441$.

Notiamo che l'espressione del MCD (a, b) fornita dall'identità di Bezout non è affatto unica.

Per dimostrare l'esistenza dell'identità di Bezout 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:

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

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}. In essa, sostituiamo il resto r_{n-1} con l'espressione $r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$ 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, ottenendo una espressione di d nei termini di r_{n-4} e r_{n-3}. Si continua, utilizzando, in ordine inverso, tutte le equazioni.
Al termine, si ottiene una espressione di d = MCD(a,b) della forma cercata.

Esercizi

1) Calcola l'identità di Bezout per MCD (1637,31)
2) Calcola l'identità di Bezout per MCD (1763,51)
3) Calcola l'identità di Bezout per MCD (1547,560)

Come trovare l'inverso in $\mathbf{Z}_n$

Sappiamo che la classe resto $\bar{a}$ in $\mathbf{Z}_n$ è invertibile se e solo se MCD(a,n)=*1*. Ma, se MCD(a,n)=1, allora, in base alla relazione di Bezout, esistono interi s e t tali che

$$1 = s \cdot a + t \cdot n .$$

Prendendo le classi modulo n, scopriamo che

$$\bar{1} = \bar{s} \cdot \bar{a} + \bar{t} \cdot \bar{n} = \bar{s} \cdot \bar{a} + \bar{t} \cdot \bar{0} = \bar{s} \cdot \bar{a}$$

Dunque $\bar{a}$ è invertibile, e $\bar{s}$ è il suo inverso.

Esempio: Siano n = 4891 e a = 2231. Per calcolare l'inverso $\bar{a}$ di modulo n, iniziamo calcolando MCD (n, a). Poiché

4891 = 2231· 2 + 429
2231 = 429 · 5 + 86
429 = 86 ·4 + 85
86 = 85 ·1 + 1

ricaviamo che MCD (n, a) = 1, e dunque la classe è effettivamente invertibile. Per calcolare l'inverso, calcolo l'identità di Bézout. Inizio evidenziando i resti nelle divisioni precedenti:

429=4891 - 2231· 2
86=2231 - 429 · 5
85=429 - 86 ·4
1= 86 - 85 ·1

e ricavo che

1 = 86 - 85 ·1 = 86 – (429 - 86 ·4) ·1= 86 ·5 - 429 · 1=
= (2231 - 429 · 5) ·5 - 429 · 1=2231 · 5- 429 · 26=
=2231 · 5- (4891 - 2231· 2) · 26= - 4891 · 26 + 2231· 57

dunque 1 = - 4891 · 26 + 2231· 57

Modulo 4891, si ha quindi che l'inverso della classe $\bar{a} = \bar{2231}$ è la classe $(\bar{a})^{-1} = \bar{57}$.

Esercizi. Verifica che $\bar{a}$ è invertibile modulo n e calcola la classe inversa per
n= 3091 , a= 2748
n= 6297 , a= 2863

Cifratura a blocchi

L'operazione di cifratura a blocchi sfrutta il fatto che l'alfabeto in chiaro sia formato da numeri (tutti della stessa lunghezza). Modifico la corrispondenza inizialmente proposta tra alfabeto e numeri, facendo in modo che i numeri utilizzati siano formati dallo stesso numero di cifre:

a	b	c	d	e	f	g	h	i	l
00	01	02	03	04	05	06	07	08	09

m	n	o	p	q	r	s	t	u	v	z
10	11	12	13	14	15	16	17	18	19	20

Ogni parola viene trasformata in una sequenza di coppie di numeri.
Comunque fissato una potenza naturale n di 10 , raggruppo le cifre in blocchi ottenuti a partire da sinistra in modo da avere sempre numeri < n.

Ad esempio, per $n = 10000 = 10^4$, raggruppo 4 cifre alla volta (corrispondenti a due lettere dell'alfabeto).
Si osservi che dai blocchi così ottenuti è possibile ricostruire l'informazione iniziale in modo perfetto: basta suddividere in coppie il blocco (partendo da sinistra).
Per cifrare, usiamo come alfabeto in chiaro i blocchi, che vivono in $\mathbf{Z_n}$. Cifriamo i singoli blocchi: chi decifra ritroverà il blocco in chiaro, e procederà a suddividerlo per ritrovare le cifre iniziali.
Non è necessario rispettare la suddivisione in coppie nella formazione dei blocchi: ad esempio posso formare blocchi di lunghezza dispari.
Per fare in modo che tutti i blocchi da cifrare abbiano la stessa lunghezza, occorre talora modificare il messaggio di partenza (aggiungendo lettere come x,y,z che possano essere facilmente riconosciute come lettere accessorie dal destinatario).
Esempio

1. Trascrivi la seguente frase passando dalle lettere ai numeri. Elimina gli spazi e dividi in blocchi di 6 cifre; se è necessario, per ottenere blocchi tutti della stessa lunghezza aggiungi la lettera z alla fine del messaggio.
   La frase è:

v	o	l	e	r	e		o		p	o	t	e	r	e

   Ottieni

v	o	l	e	r	e		o		p	o	t	e	r	e
19	12	09	04	15	04		12		13	12	17	04	15	04

   Da cui la stringa da suddividere 191209041504121312170415042020
   cui aggiungo 2020 (cioè zz) per poter suddividere i blocchi di uguale lunghezza 6. Ottengo i blocchi 191209 041504 121312 170415 042020
   Osserviamo che stiamo lavorando in $Z_{1000000}$ e la chiave cifrante è [888889]; ricaviamo il messaggio cifrato

   080098 930393 010201 059304 930909

2. Ora cifra il messaggio, con un cifrario di Cesare di chiave cifrante 888889.
   Ottieni .....

2. Decifra il messaggio seguente, che è stato suddiviso in blocchi di 6 cifre e cifrato con un cifrario di Cesare, di chiave cifrante [888889]: messaggio 060393 919691 969197 049306 059299 890393

Osserviamo che stiamo lavorando in $Z_{1000000}$ e la chiave cifrante è
[888889] = – [111111] : dunque, per decifrare basta sommare [111111] oppure sottrarre [888889] ad ogni blocco, ottenendo:
171504 030802 080308 160417 170410 011504
e poi dividere i numeri ottenuti in blocchi di 2 cifre:

17	15	04	03	08	02	08		03	08		16	04	17	17	04	10	01	15	04
t	r	e	d	i	c	i		d	i		s	e	t	t	e	m	b	r	e

Esercizi

1. Scrivi a blocchi di 5 cifre il messaggio 'vento da sud', poi cifralo con un sistema affine di chiave ($\bar{a} = \bar{3}$, $\bar{b} = \bar{349}$). Determina in modo esplicito la funzione per decifrare.
2. Decifra il messaggio cifrato (con blocchi di 5 cifre) con il sistema affine di chiave ($\bar{a} = \bar{27027}$, $\bar{b} = \bar{349}$). Messaggio: = 78027 12116 35080 54300