Numeri e crittografia

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

1. Sistema crittografico di Cesare e introduzione all'aritmetica modulare

2. Sistemi crittografici e cifratura a blocchi

3. Prodotto tra classi resto e cifrari affini

4. Classi invertibili, massimo comune divisore e algoritmo di Euclide

5. Potenze di classi resto e cifrari a chiave pubblica

Numeri e crittografia

1. Sistema crittografico di Cesare e introduzione all'aritmetica modulare

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 d el 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

Per esempio, se il messaggio da inviare è il seguente:
torno domani
il risultato dopo la cifratura sarà:
ZRUQR GRPDQN

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 del 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.

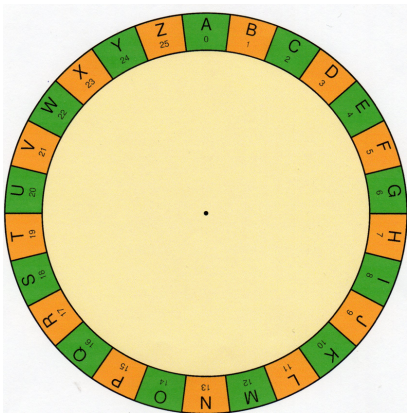
v	i	e	n	i		a	l		m	a	r	e	?						

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 ……

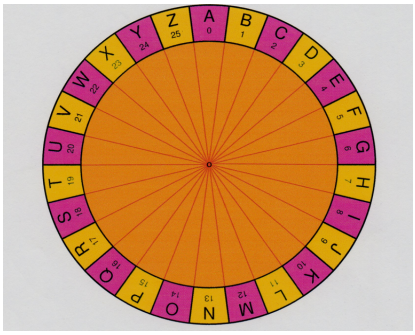
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z

O	A	V	L	Z	T		B	T	A	H	P								

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 (vedi figura). Sovrapponendo i due cerchi, è possibile far ruotare l'alfabeto cifrante in base alla chiave di Cesare fissata e ottenere la legge di cifratura.



L'alfabeto in chiaro



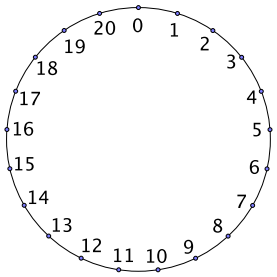
L'alfabeto cifrante (su un cerchio più piccolo)

Cerchiamo di interpretare la procedura seguita: assegniamo a ogni lettera dell'alfabeto italiano in chiaro un numero corrispondente alla sua posizione come nella seguente tabella 1:

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

e disponiamo le lettere (e i corrispondenti numeri) come ore su un orologio (vedi figura). Ogni lettera viene identificata come una posizione sull'orologio, e l'orologio ha 21 'ore':



Decidiamo un numero (ad esempio 5) che rappresenta la nostra chiave. La rotazione di 5 posizioni in senso antiorario 'corrisponde' a sommare + 5 a ogni numero dell'alfabeto in chiaro? se sommiamo 5 a ogni posizione, nell'alfabeto cifrante

la $a \Leftrightarrow 0$ corrisponde alla lettera in posizione 5 cioè alla F,
la $b \Leftrightarrow 1$ alla G $\Leftrightarrow 6$,
…,
la $r \Leftrightarrow 15$ alla Z $\Leftrightarrow 20$.

La $s \Leftrightarrow 16$ corrisponde però alla A$\Leftrightarrow$0, la $t \Leftrightarrow 17$ alla B$\Leftrightarrow$1, …, la $z \Leftrightarrow 20$ alla E$\Leftrightarrow$5.
Per descrivere le scelte fatte, possiamo ragionare nel modo seguente, ricordando che

- la lettera *t* occupa la posizione 17 (ricorda che partiamo dalla posizione 0) e nella rotazione operata si sposta nella posizione 1
- $17+5=22$ e $22 = 1 \cdot 21 + 1$
- Possiamo dire che 22 corrisponde alla posizione 1, immaginando di aver fatto un giro completo, ma tenendo conto solo della posizione di arrivo.

Allo stesso modo, la lettera *s* corrisponde alla A (perché *s*⇔16, 16+5=21, 21 = 1 · 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) e, 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. Nelle 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*.

Esercizio 1) Seguendo l'esempio, determina un numero tra 0 e *n*-1 congruente modulo *n* al numero assegnato:

- 23 è congruente modulo 21 a 2
- 30 è congruente modulo 21 a .....
- 40 è congruente modulo 21 a .....
- – 1 è congruente modulo 21 a .....
- 58 è congruente modulo 21 a .....

2) È vero che 132 è congruente a 257 modulo 21?

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,

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

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

Esempi:

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

Osservazioni sulle proprietà della congruenza

1. Ogni numero è congruente a se 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 precedenti 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 suddivide quindi gli interi in sottoinsiemi tra loro disgiunti:

Definizione Dato $a \in \boldsymbol{Z}$, denotiamo con $\overline{a}$ l'insieme

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

Diciamo che a **rappresenta** la classe resto (o **è rappresentante della classe resto**).
Diciamo anche che $\overline{a}$ è a modulo *21* (in simboli*: a mod 21*).
Useremo qualche volta anche il simbolo *[a]* per denotare la classe resto rappresentata da a mod n. 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 a uno e a uno solo tra i numeri 0, … , $n-1$. Dunque, **le classi resto modulo *n* sono esattamente *n* e ciascuna di esse ha uno e un solo rappresentante in**

$$\{ 0, 1, 2, ..., n-1 \} .$$

Cercheremo di usare sempre il rappresentante della classe scelto con questo criterio.

Esempio Calcoliamo 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

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

Ricordiamo la Tabella 1:

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

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

$$0 \le b \le n–1$$

Come in $\mathbf{Z}$, 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 rappresentato da $\mathscr{P} = \mathbf{Z}_{21}$.

16≡31 mod 5	V□ F□
25≡13 mod 13	V□ F□
72≡-21 mod 31	V□ F□
82≡59 mod 29	V□ F□

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 di Cesare (che viene anche detto sistema 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 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

2. Sistemi crittografici e cifratura a blocchi

Sistemi crittografici

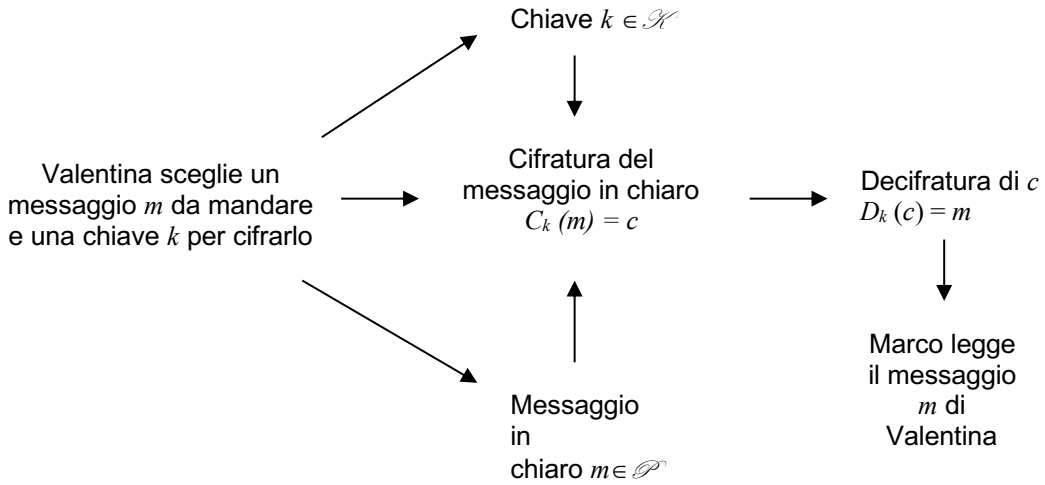
Discutiamo più in generale la nozione di crittografia.
La **cifratura** è una operazione di passaggio da un messaggio (detto **messaggio in chiaro**) ad un messaggio il cui significato è "nascosto" (detto **messaggio cifrato**): ad esempio il passaggio da un linguaggio ad un altro poco diffuso.

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, ad esempio, cifrare singole parole (basta pensare ad un vocabolario inglese-italiano) 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 a elementi distinti di A corrispondono elementi distinti di B. È suriettiva se ogni elemento di B è immagine di almeno un elemento del dominio 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

Elementi critici nel cifrario di Cesare (e nei cifrari monoalfabetici)
Se intercettiamo un messaggio che sappiamo essere stato criptato col metodo di Cesare, possiamo sicuramente decifrarlo se scopriamo quanto vale la chiave k utilizzata. Talora è però possibile decodificare un messaggio pur non conoscendo la chiave k.
Procedere per tentativi è in generale poco efficace: nel caso del cifrario di Cesare, ad esempio, i cifrari possibili sono 20 nel caso di un testo scritto in lingua italiana (25 se il testo è in inglese). Ma i tempi di decifratura potrebbero essere troppo lenti.
Uno strumento essenziale è l'analisi del testo. Poiché nella lingua italiana la maggior parte delle parole termina con una delle vocali *a, e, i, o* vorrà dire che le lettere finali delle parole del messaggio cifrato hanno una maggiore probabilità di essere una di queste lettere. Nel prossimo paragrafo, vedremo come eludere questa considerazione spezzando il messaggio in blocchi della stessa lunghezza il che rende complicata la ricostruzione delle singole parole.

Però si può ricorrere ad altre considerazioni. Se nel testo ci sono lettere consecutive identiche all'interno della stessa parola, queste probabilmente sono consonanti. Inoltre, come osservato anche da Leon Battista Alberti, in ogni lingua ci sono lettere che compaiono nei testi con maggiore frequenza ed altre più raramente; ad esempio nella lingua italiana le lettere più frequenti sono nell'ordine *e, a, i* mentre le meno usate sono *q, z*. Altre informazioni si possono reperire dalla frequenza delle doppie, dalla tendenza di certe lettere a non gradire la vicinanza di altre, ecc.
Riportiamo di seguito una tabella riassuntiva delle frequenze nella lingua italiana (in un linguaggio non tecnico e in testi non appositamente costruiti per eludere l'analisi delle frequenze).

%	Lettera	%	Lettera	%	Lettera
11,79	*e*	*5,63*	t	2,10	v
11,74	*a*	*4,98*	s	1,65	g
11,28	*i*	*4,50*	c	1,54	h
9,83	*o*	*3,73*	d	0,95	f
6,88	n	*3,05*	p	0,92	b
6,51	l	*3,02*	u	0,51	q
6,38	r	*2,52*	m	0,49	z

Tavola delle frequenze lingua italiana

Supponiamo di intercettare il seguente messaggio:
TQ FZZB MFIEQEF BE SBISFCF MNMMU CU OUMMNIU, QESAU HNUCCU GBN BEHNBEQEMB. DQ TFDQEB CQ SBMMQ LB VUIDQ. TFGF OUEMBLUMMU ZBFIEB TB CBOUCCB TB LDFZ VNFIBCUZZU, SAU IUETFEF BC ZUEEQBF QGGUEQ SFESlNLF BC GUZZBFI DULU EUZCB NCMBDB TBUSB QEEB, CQ HNQCBMQ TUCC QIBQ U DBZCBFIQMQ CBUOUDUEMU
e di voler scoprire cosa significhi.
Riportiamo la frequenza delle lettere nel nostro messaggio

Lettera	Occorrenze	Lettere	Occorrenze	Lettera	Occorrenze
A	2	H	3	Q	19
B	34	I	10	R	0
C	19	L	5	S	8
D	8	M	18	T	8
E	20	N	8	U	28
F	18	O	4	V	2
G	5	P	1	Z	11

Le lettere con maggiore frequenza (in ordine decrescente di frequenza) sono: B, U, C (compare come doppia), E (compare come doppia), Q, F.
Le lettere terminali di una parola, in ordine decrescente di frequenza, sono B (9), U (8), C (3, compare come doppia), E (1, compare come doppia), Q (9), F (5), Z, I, N: nella parentesi è indicata la frequenza come terminale di parola.
Le lettere che compaiono come doppie sono: E, C, M, Z.
Primo tentativo: inizio dalle lettere B, U, Q terminali di una parola e associando loro vocali, tenendo conto delle osservazioni svolte; vista la differenza elevata tra la frequenza di B e di U e Q, iniziamo sostituendo le consonanti E = n, C = l.

Si ottiene
TQ FZZB MFInQnF Bn SBISFlQPBFnU MNMMU lU OUMMNIU, QnSAU HNUllU GBN BnHNBnQnMB. DQ TFDQnB CQ SBMMQ LB VUIDQ. TFGF OUnMBLUMMU ZBFInB TB lBOUllB TB LDFZ VNFIBlUZZU, SAU IUnTFnF Bl ZUnnQBF QGGUnQ SFnSlNLF Bl GUZZBFI DULU nUZCB NlMBDB TBUSB QnnB, lQ HNQlBMQ TUll QIBQ U DBZlBFIQMQ lBUOUDUnMU

Le parole *Bn, Bl* e *QnnB* e la presenza di dittonghi suggeriscono la sostituzione B = i, U = e , Q = a . Otteniamo:

Ta FZZi MFInanF in SiISFlaPiFne MNMMe le OeMMNIe, anSAe HNelle GiN inHNinanMi. Da TFDani Ca SiMMa Li VeIDa. TFGF OenMiLeMMe ZiFIni Ti liOelli Ti LDFZ VNFIileZZe, SAe IenTFnF il ZennaBF aGGeEa SFnSlNLF il GeZZiFI DeLe neZCi NlMiDi TieSi anni, la HNaliMa Tell aIia e DiZliFIaMa lieOeDenMe

Proviamo a inserire un'altra vocale: F = o
Ta oZZi MoInano in SiISolaPioEe MNMMe le OeMMNIe, anSAe HNelle GiN inHNinanMi. Da ToDani Ca SiMMa Li VeIDa. ToGo OenMiLeMMe ZioIni Ti liOelli Ti LDoZ VNoIileZZe, SAe IenTono il ZennaBo aGGeEa SonSlNLo il GeZZioI DeLe neZCi NlMiDi TieSi anni, la HNaliMa Tell aIia e DiZlioIaMa lieOeDenMe

Ora, la sostituzione M = r non sembra opportuna, e si preferisce quindi M = t, ottenendo
Ta oZZi toInano in SiISolaPioEe tNtte le OettNIe, anSAe HNelle GiN inHNinanti. Da ToDani Ca Sitta Li VeIDa. ToGo OentiLette ZioIni Ti liOelli Ti LDoZ VNoIileZZe, SAe IenTono il ZennaBo aGGeEa SonSlNLo il GeZZioI DeLe neZCi NltiDi TieSi anni, la HNalita Tell aIia e DiZlioIata lieOeDente

Ora, le lettere più frequenti non ancora sostituite sono Z, I e N, S, T, D: si verifica se sia possibile sostituirle con r, s, c, d. La parola *oZZi* rende apparentemente inopportuna la sostituzione Z=r; si prova quindi la sostituzione I = r, ottenendo
Ta oZZi tornano in SirSolaPioEe tNtte le OettNre, anSAe HNelle GiN inHNinanti. Da ToDani Ca Sitta Li VerDa. ToGo OentiLette ZioIni Ti liOelli Ti LDoZ VNoIileZZe, SAe IenTono il ZennaBo aGGeEa SonSlNLo il GeZZior DeLe neZCi NltiDi TieSi anni, la HNalita Tell aria e DiZliorata lieOeDente

Ormai il testo produce indizi: ad esempio, le sostituzioni S = c, N = u che forniscono
Ta oZZi tornano in circolaPioEe tutte le Oetture, anSAe HNelle GiN inHuinanti. Da ToDani Ca Sitta Li VerDa. ToGo OentiLette ZioIni Ti liOelli Ti LDoZ VuoIileZZe, SAe IenTono il ZennaBo aGGeEa conclNLo il GeZZior DeLe neZCi ultiDi Tieci anni, la Hualita Tell aria e DiZliorata lieOeDente

Si procede con successive scelte, che vengono eventualmente riviste, ricavando il testo in chiaro
Da oggi tornano in circolo tutte le vetture, anche quelle più inquinanti. Ma domani la città si ferma. Dopo 27 giorni di livelli di smog fuorilegge, che rendono il gennaio appena concluso il peggior mese negli ultimi dieci anni, la qualità dell'aria è migliorata lievemente

È chiaro che il modo di procedere è molto falsato perché stiamo facendo l'analisi di un testo troppo breve, ma l'importante è aver sottolineato come le tante possibilità teoriche possano essere notevolmente ridotte usando informazioni sul linguaggio e procedendo sistematicamente per tentativi.
L'analisi delle frequenze rende fragile qualsiasi sistema crittografico che cifra una lettera alla volta, e la cifra sempre nello stesso modo. Il paragrafo successivo illustra un metodo che riduce la possibilità di utilizzare l'analisi delle frequenze.

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 191209041504121312170415 04

cui aggiungo 2020 (cioè zz) per poter suddividere i blocchi di uguale lunghezza 6. Ottengo i
blocchi 191209 041504 121312 170415 042020
Ora cifriamo il messaggio, con un cifrario di Cesare di chiave cifrante 888889. Osserviamo che stiamo lavorando in $Z_{1000000}$ e la chiave cifrante è [888889]; ricaviamo il messaggio cifrato
080098 930393 010201 059304 930909

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

3. Prodotto tra classi resto e cifrari affini

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: *se non si utilizzano macchine cifranti, è più facile non commettere errori quando la cifratura si può effettua secondo una regola semplice da memorizzare.*
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 In $\mathbf{Z}_n$ sono definite due operazioni. Date due classi resto $\bar{a}$ e $\bar{b}$ modulo *n*, si pone:

- la somma di classi: $\bar{a}+\bar{b} = \overline{a+b}$ (conosciamo già questa operazione)
- il prodotto di classi: $\bar{a} \times \bar{b} = \overline{a \times b}$

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 = 4·9+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.

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

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 sempre vale in $\mathbf{Z}_n$.; ad esempio:

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

Esercizio Completare le tavole dei prodotti

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						

Modulo 9

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

Soluzione

Modulo 5

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

Modulo 6

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

Modulo 9

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

Applicazioni del prodotto alla crittografia

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 $\bar{5}$:

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Aritmetica modulare e crittografia
Russell, dicembre 2019-gennaio 2020

	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

La legge di cancellazione $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{c} \Rightarrow \bar{b} = \bar{c}$ vale in $\mathbf{Z}$ purché sia $a \neq 0$, *ma* non sempre vale in $\mathbf{Z}_n$.; ad es., $3 \cdot 5 \equiv 3 \cdot 8 \equiv 6 \bmod 9$ 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 6 modulo 9.

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

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*

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

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

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

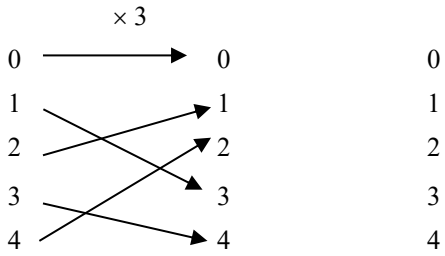
Abbiamo trovato un assurdo (perché la moltiplicazione non sarebbe iniettiva), quindi *MCD (a,n) =1.* ◊

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

Classi resto invertibili

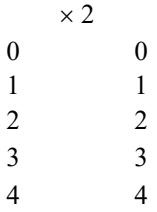
Ora sappiamo come scegliere la classe $\bar{a}$ in modo che la moltiplicazione per $\bar{a}$ sia una funzione cifrante: ma come decifrare?

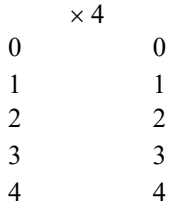
1. **Esercizio** Abbiamo visto che **la moltiplicazione per 3, modulo 5,** è iniettiva. Costruisci con le frecce la corrispondente funzione inversa:

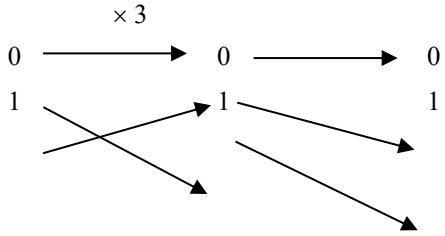


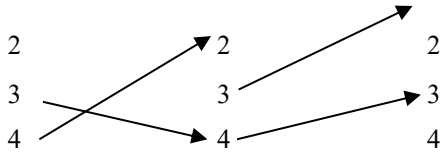
2. Controlla se la funzione inversa coincide con la moltiplicazione, modulo 5, per uno di questi numeri: 2, 3, 4.

Soluzione **1.**

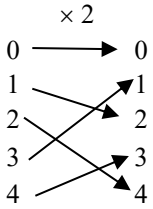


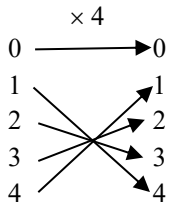






2. La funzione inversa coincide con la moltiplicazione per 2.





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.

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

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

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* $\mathrm{MCD}(a,n) = 1$.

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

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

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:

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

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

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

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.

4. Classi invertibili, Massimo comune divisore e algoritmo di Euclide

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*.

Proprietà della divisibilità

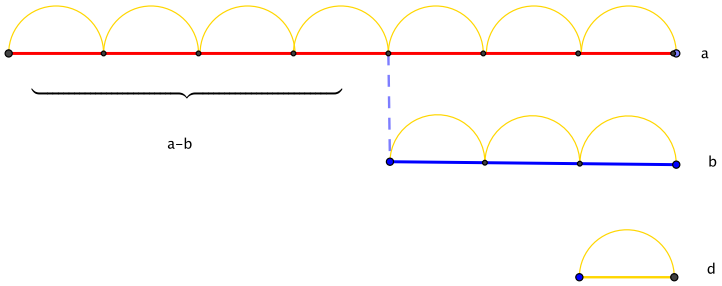
- **Riflessiva**: d è divisore di d
- **Antisimmetrica**: se d è divisore di a e a è divisore di d allora $a = d$

$$\left.\begin{matrix} d|a \\ a|d \end{matrix}\right\} \Longrightarrow d = a$$

- **Transitiva**: siano a, b, $d \neq 0$; se d è divisore b e b è divisore di a allora d è divisore di a

$$\left.\begin{matrix} d|b \\ b|a \end{matrix}\right\} \Longrightarrow d|a$$

- Se d è divisore di a e d è divisore di b, allora d è divisore di (a +b) e di (a – b)

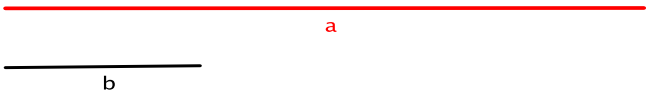


- **L'insieme dei divisori comuni di *a* e *b* coincide con l'insieme dei divisori comuni di *a-b* e *b***

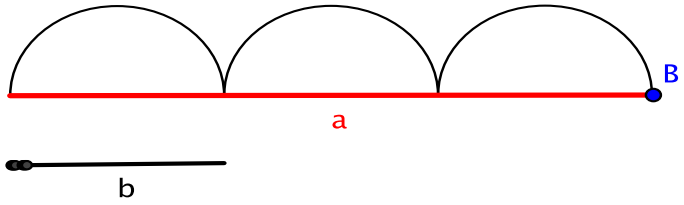
La divisione tra numeri naturali può essere riletta nel modo seguente:
Proposizione Siano a, b numeri na turali non nulli. Allora esistono e sono univocamente determinati due interi q e r tali che

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

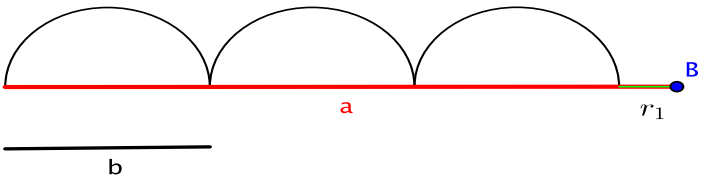
In quest'operazione a è detto *dividendo*, b *divisore*, q *quoziente* e r *resto.*
L'**algoritmo di Euclide** (o **metodo delle divisioni successive**) consente di calcolare il MCD tra due qualsiasi numeri e si basa su una serie di divisioni successive.
Siano dati due numeri naturali a e b, di cui si vuole calcolare il massimo comune divisore MCD(a,b). Supponiamo che $a > b$ e rappresentiamo i numeri a e b come lunghezze di un segmento:



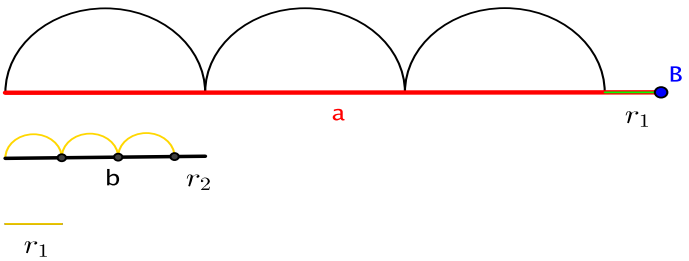
Dividendo a per b e si ottengono un quoziente q_1 e un resto r_1, con $a = b \cdot q_1 + r_1$.
Se $r_1 = 0$, allora ***a* è multiplo di *b***



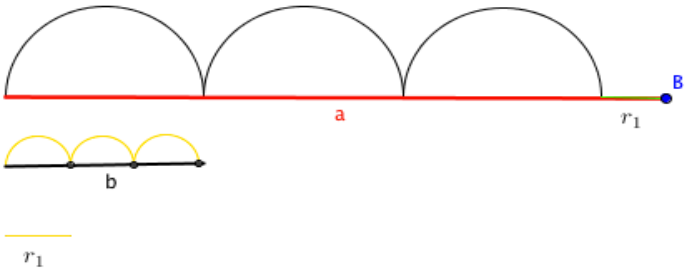
quindi MCD $(a,b)=b$ e ci si ferma;
se $r_1 \neq 0$, allora ***a* non è multiplo di *b*.**



Il resto r_1 individua un nuovo segmento, minore di b: lo aggiungo nel disegno, colorandolo in giallo. Provo a dividere b per r_1, ottenendo un quoziente q_2 e un resto r_2;



Se $r_2 = 0$, la situazione è come in figura:



Sappiamo che r_1 divide b, cioè b è multiplo di r_1 . Ma allora r_1 divide anche a ed è un divisore comune di a e b. Ma qualsiasi divisore comune di a e b deve dividere r_1 .
Concludiamo che r_1 = **MCD(*a,b*) e osserviamo che r_1 è l'ultimo resto non nullo**.
Se, invece, $r_2 \neq 0$, si ripete il ragionamento:
- disegniamo un nuovo segmento di lunghezza r_2
- dividiamo 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 è sempre maggiore o uguale a 0, ma si riduce ad ogni passo.

Ricordiamo che l'insieme dei divisori comuni di *a* e *b* coincide con l'insieme dei divisori comuni di *a-b* e *b* : quindi, ad ogni passo, non si modifica l'insieme dei divisori comuni delle coppie utilizzate, e in particolare non si modifica il loro massimo comune divisore.

Esempio Il procedimento è illustrato di seguito, calcolando MCD (44880,5292).

$44880 = 5292 \cdot 8 + 2544$

$5292 = 2544 \cdot 2 + 204$

$2544 = 204 \cdot 12 + 96$

$204 = 96 \cdot 2 + \mathbf{12}$

$96 = 12 \cdot 8 + 0$ ← MCD

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

Esempi
1) Calcola MCD (1637,31)

$1637 = 31 \cdot 52 + 25$
$31 = 25 \cdot 1 + 6$
$25 = 6 \cdot 4 + 1$ ← MCD
$6 = 1 \cdot 6 + \mathbf{0}$

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

2) Calcola MCD (1763, 51)

$1763 = 51 \cdot 34 + 29$
$51 = 29 \cdot 1 + 22$

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 **IDENTITÀ DI BÉZOUT**.

Vediamo il procedimento per trovare un'identità di Bézout 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 mettendo in evidenza i resti non nulli, nel modo seguente:

$44880 = 5292 \cdot 8 + 2544 \quad \rightarrow \quad r_1 = 2544 = 44880 - 5292 \cdot 8$
$5292 = 2544 \cdot 2 + 204 \quad \rightarrow \quad r_2 = 204 = 5292 - 2544 \cdot 2$
$2544 = 204 \cdot 12 + 96 \quad \rightarrow \quad r_3 = 96 = 2544 - 204 \cdot 12$
$204 = 96 \cdot 2 + 12 \quad \rightarrow \quad \text{MCD} = r_4 = 12 = 204 - 96 \cdot 2$

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 una espressione nei numeri a, b. I numeri colorati vanno trattati come se fossero lettere, mentre si svolgono i calcoli che coinvolgono i loro coefficienti. Otteniamo:

$$\begin{aligned} 12 &= 204 - 96 \cdot 2 = 204 - (2544 - 204 \cdot 12) \cdot 2 = \\ &= 204 - 2544 \cdot 2 - 204 \cdot 24 \\ &= 204 \cdot 25 - 2544 \cdot 2 = (5292 - 2544 \cdot 2) \cdot 25 - 2544 * 2 \\ &= 5292 \cdot 25 - 2544 \cdot 52 = 5292 \cdot 25 - (44880 - 5292 \cdot 8) \cdot 52 \\ &= 5292 \cdot 441 - 44880 \cdot 52 \end{aligned}$$

$$12 = 441 \cdot 5292 - 52 \cdot 4480$$

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, 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 di $\bar{a}$ 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 $\bar{a}$ è effettivamente invertibile. Per calcolarne l'inverso, determiniamo l'identità di Bézout. Evidenziamo i resti nelle divisioni precedenti:

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

e ricaviamo 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

Tavola di lavoro

1. Utilizzando il metodo delle divisioni successive, calcola MCD(1637, 31)

a	b	resto

a	=	b	×	quoziente	+	resto
	=		×		+	
	=		×		+	
	=		×		+	
	=		×		+	

MCD(1637, 31) = ……

2. Ricostruisci ora l'identità di Bezout:

MCD=	=		=	
	=		=	
	=		=	
	=		=	
	=		=	

In conclusione, si può scrivere:

……	=	……	*	1637	+	……	*	31
MCD	=	s	*	a	+	t	*	b

3. Passando alle classi resto, l'inverso di 31 modulo 1637 è ……..

Soluzione della tavola di lavoro

1. Utilizzando il metodo delle divisioni successive, calcola MCD(1637, 31)

a	b	resto
1637	31	25
31	25	6
25	6	**1**
6	1	0

a	=	b	*	quoziente	+	resto
1637	=	31	*	52	+	25
31	=	25	*	1	+	6
25	=	6	*	4	+	**1**
6	=	1	*	6	+	

MCD(1637, 31) = 1

2. Ricostruisci ora l'identità di Bezout:

MCD=1	=	25–6*4	=	25 – (31 – 25*1) *4
	=	25–31*4+25*4	=	25*5 – 31*4
	=	(1637–31*52)*5 – 31*4	=	1637*5–31*260–31*4
	=	1637*5 –31* 264	=	

In conclusione, si può scrivere:

1	=	5	*	1637	+	(–264)	*	31
MCD	=	s	*	a	+	t	*	b

3. Quindi l'inverso di 31, modulo 1637, è $[-264] = [1373]$

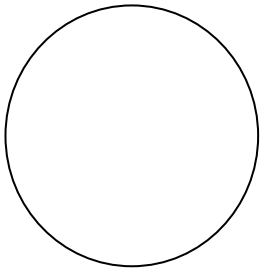
Tavola di lavoro

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

Tavola di lavoro
Le chiavi e gli elementi invertibili quando *n* è primo

1. Quante sono le chiavi per cifrare con la moltiplicazione
   $p \to \bar{a} \cdot \bar{p}$ modulo 5?
   Sono ....
   Rappresenta $\mathbf{Z}_5$ sul cerchio, mettendo in evidenza le classi invertibili.

Invertibile?	si	no
0		
1		
2		
3		
4		



2. Supponiamo che *n* sia primo: quanti sono i numeri *a* compresi tra 1 e *n* che sono coprimi con *n*, cioè tali che
   $$\text{MCD}(a, n) = 1 \ ?$$
   Sono .....
3. Se *n* è primo, quanti sono gli elementi invertibili di $\mathbf{Z}_n$? Sono .....
4. Se *n* è primo, quante sono le chiavi per cifrare con la moltiplicazione
   $$p \to \bar{a} \cdot \bar{p} \text{ modulo } n?$$
   Sono .....

5. Quante sono le chiavi per cifrare con la moltiplicazione
   $$p \to \bar{a} \cdot \bar{p} \text{ modulo } 6?$$

Sono ....

Soluzione tavola di lavoro Le chiavi e gli elementi invertibili quando *n* è primo

1. Le chiavi per cifrare con la moltiplicazione $p \to \bar{a} \cdot \bar{p}$ modulo 5 sono 4.
   Sono ....

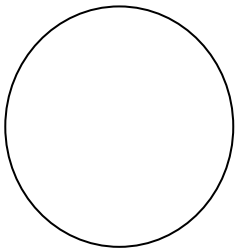
Invertibile?	si	no
0		x
1	x	
2	x	
3	x	
4	x	

2. Supponiamo che *n* sia primo: quanti sono i numeri *a* compresi tra 1 e *n* che sono coprimi con *n*, cioè tali che MCD$(a, n) = 1$? Sono $n - 1$
3. Se *n* è primo, quanti sono gli elementi invertibili di $\mathbf{Z}_n$? Sono $n - 1$
4. Se *n* è primo, quante sono le chiavi per cifrare con la moltiplicazione $p \to \bar{a} \cdot \bar{p}$ modulo *n*?
   Sono $n - 1$ (anche se la chiave 1 non è conveniente da utilizzare)

tavola di lavoro Le chiavi e gli elementi invertibili quando *n* è prodotto di due primi distinti

Quante sono le chiavi per cifrare con la moltiplicazione $p \to \bar{a} \cdot \bar{p}$ modulo 6?
Rappresenta $\mathbf{Z}_6$ sul cerchio, mettendo in evidenza le classi invertibili.

Invertibile?	si	no
0		
1		
2		
3		
4		
5		



1. Fai l'elenco dei numeri a con $0<a<15$ e tali che MCD$(a,3)>1$: {……}. Sono ……..

Fai l'elenco dei numeri a con $0<a<15$ e tali che MCD$(a,5)>1$: {……}. Sono ……..
Fai l'elenco dei a, con $0<a<15$, tali che MCD$(a,15)>1$: {……}. Sono ……..

Ricorda che gli invertibili in $\mathbf{Z}_{15}$ sono i numeri a con $0<a<15$ e tali che MCD$(a, 15)=1$. A partire da quanto hai osservato, quanti sono gli invertibili in $\mathbf{Z}_{15}$?
Sono .....

2. Sia n il prodotto di due primi distinti:

$n = p\,q$ con p e q primi distinti

a) Quanti sono i numeri a con $0<a<n$ che sono divisibili per p? Sono .....
b) Quanti sono i numeri a con $0<a<n$ che sono divisibili per q? Sono .....
c) Quanti sono i numeri a, con $0<a<n$, che NON sono coprimi con n? Sono .....
d) Quanti sono gli elementi invertibili in $\mathbf{Z}_n$? Sono .....

Soluzione tavola di lavoro

1. Le chiavi per cifrare con la moltiplicazione $p \to \bar{a} \cdot \bar{p}$ modulo 6 sono 2.

Invertibile?	si	no
0		x
1	x	
2		x
3		x
4		x
5	x	

1. I numeri a con $0<a<15$ e tali che MCD$(a,3)>1$ sono {3, 6, 9, 12}. Sono 4.
I numeri a con $0<a<15$ e tali che MCD$(a,5)>1$ sono {5, 10}. Sono 2.
I numeri a, con $0<a<15$, tali che MCD$(a,15)>1$ sono {3, 6, 9, 12, 5, 10}. Sono 6

Ricorda che gli invertibili in $\mathbf{Z}_{15}$ sono i numeri a con $0<a<15$ e tali che MCD$(a, 15)=1$. A partire da quanto hai osservato, quanti sono gli invertibili in $\mathbf{Z}_{15}$? Sono 6

2. Sia n il prodotto di due primi distinti: $n = p\,q$ con p e q primi distinti

a) I numeri a con $0<a<n$ che sono divisibili per p sono $q - 1$
b) I numeri a con $0<a<n$ che sono divisibili per q sono $p - 1$
c) I numeri a, con $0<a<n$, che NON sono coprimi con n sono $(n-1) - (q - 1) - (p - 1) = n - q - p + 1$
d) Gli elementi invertibili in $\mathbf{Z}_n$ sono $n-q-p-1 = pq-q-p-1 = p(q-1) - (q-1) = (p-1)(q-1)$

5. Potenze di classi resto e cifrari a chiave pubblica

Le potenze

Utilizzando le operazioni in $\mathbf{Z}_n$, è possibile cercare altre cifrature. Cosa succede se, per cifrare, elevo ogni elemento ad una potenza fissata? Sto considerando l'applicazione:

$$\mathbf{Z}_n \to \mathbf{Z}_n \text{ definita da: } x \to x^t$$

Sono trasformazioni accettabili come cifrature?

Provo ad elevare al quadrato **Modulo 10**:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\mathbf{x^2}$	**0**	**1**	**4**	**9**	**6**	**5**	**6**	**9**	**4**	**1**

L'elevamento al quadrato non è una trasformazione iniettiva e suriettiva.
C'è un esponente corretto da usare per ottenere una funzione iniettiva?

Tavola di lavoro Le potenze in Z_5.

Ricorda la tavola del prodotto modulo 5:

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

Consideriamo la funzione f_m: $\mathbf{Z}_5 \to \mathbf{Z}_5$ tale che $f_m : x \to x^m$

Vogliamo scoprire per quale valore di m la funzione f_m è una funzione di cifratura.

Completa la tabella dei valori corrispondenti delle potenze di x.

Per calcolare velocemente le potenze di un elemento, ricorda che

$$x^m x^n = x^{m+n}$$

$$(x^m)^n = x^{m\,n}$$

	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
0	0									
1	1									
2	2									
3	3									
4	4									

a) L'elevamento al quadrato è una cifratura? E se uso un esponente pari?
b) I valori di m per i quali la funzione f_m è una funzione di cifratura sono:
c) Ci due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Se si, quali?
d) Saresti in grado di completare la tabella seguente senza fare conti?

	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}
0					
1					
2					
3					
4					

Dopo quanti passi le funzioni si ripetono?

Soluzione tavola Le potenze in Z_5

Completa la tabella dei valori corrispondenti delle potenze di x .

	x	x^2	$x^3 = xx^2$	$x^4=(x^2)^2$	$x^5 = x^4x = x$	$x^6=x^4x^2= x^2$	$x^7= x^4x^3= x^3$	$x^8= (x^4)^2$	$x^9 = x^8x= x$	x^{10}
0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	2	4	3	1	2	4	3	1	2	4
3	3	4	2	1	3	4	2	1	3	4
4	4	1	4	1	4	1	4	1	4	1

a) L'elevamento al quadrato è una cifratura? no, perché $1^2 = 4^2$ e dunque la funzione non è iniettiva. E se uso un esponente pari? Poiché $(x^{2k}) = (x^2)^k$, elevare a una potenza pari non è mai una funzione iniettiva: quindi, non è una cifratura.

b) I valori di m per i quali la funzione f_m è una funzione di cifratura sono: 1, 3 (ma 1 corrisponde a lasciare il messaggio in chiaro)

c) Ci due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Si

Se sì, quali? Ad esempio, 2 e 6. In generale quando m è congruo a k modulo 4.

d) Saresti in grado di completare la tabella seguente senza fare conti?

	$x^{11} = x^3$	$x^{12} = x^4$	$x^{13} = x$	$x^{14} = x^2$	$x^{15} = x^3$
1	1	1	1	1	1
2	3	1	2	4	3
3	2	1	3	4	2
4	4	1	4	1	4

Dopo quanti passi le funzioni si ripetono? 4

E se consideriamo esponenti negativi? posso utilizzare esponenti negativi solo per elementi invertibili (cioè tutti tranne lo [0])

Tavola di lavoro Le potenze in Z_7

Ricorda la tavola del prodotto modulo 7 e considera la funzione

$$f_m: \mathbf{Z}_7 \to \mathbf{Z}_7$$

tale che $f_m(x) = x^m$. Vogliamo scoprire per quale valore di m la funzione f_m è una funzione di cifratura.

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

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Aritmetica modulare e crittografia
Russell, dicembre 2019-gennaio 2020

1. **Completa la tabella dei valori delle potenze di x :**

	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
0	0									
1	1									
2	2									
3	3									
4	4									
5	5									
6	6									

a) L'elevamento al quadrato è una cifratura? E se uso un esponente pari?
b) I valori di m per i quali la funzione f_m è una funzione di cifratura sono:
c) Ci due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Se sì, quali?
d) Saresti in grado di completare la tabella seguente senza fare conti? Dopo quanti passi le funzioni si ripetono?

	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}
0					
1	1				
2	4				
3	5				
4	2				
5	3				
6	6				

Soluzione Tavola di lavoro Le potenze in Z_7

	x	x^2	$x^3 = xx^2$	$x^4 = (x^2)^2$	$x^5 = x^4x$	$x^6 = (x^3)^2$	$x^7 = x^6x = x$	$x^8 = x^6x^2 = x^2$	$x^9 = x^6x^3 = x^3$	$x^{10} = x^6x^4 = x^4$
0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	2	4	1	2
3	3	2	6	4	5	1	3	2	6	4
4	4	2	1	4	2	1	4	2	1	4
5	5	4	6	2	3	1	5	4	6	2
6	6	1	6	1	6	1	6	1	6	1

a) L'elevamento al quadrato non è una cifratura perché $1^2 = 4^2$ e dunque la funzione non è iniettiva. Poiché $(x^{2k}) = (x^2)^k$, elevare a una potenza pari non è mai una funzione iniettiva: quindi, non è una cifratura.
b) I valori di m per i quali la funzione f_m è una funzione di cifratura sono: 1, 5
c) Ci due esponenti diversi m e k per i quali le funzioni f_m e f_k coincidono? Se si, quali? Si
Se sì, quali? Ad esempio, 2 e 6. In generale quando m è congruo a k modulo 6
d) Le funzioni si ripetono dopo 6 passi

	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}
1	1	1	1	1	1
2	4	1	2	4	1
3	5	1	3	2	6
4	2	1	4	2	1
5	3	1	5	4	6
6	6	1	6	1	6

Quando *n* è primo: Piccolo Teorema di Fermat

Riprendiamo la tavola del prodotto modulo 5, senza considerare l'elemento [0]. Studiando le potenze in $\mathbf{Z}_5$, abbiamo visto che, se $x \neq [0]$, allora $x^4=1$. Cerchiamo di capire meglio.

×	**1**	**2**	**3**	**4**
1	1×1=1	1×2= 2	1×3=3	1×4=4
2	2×1=2	2×2= 4	2×3=1	2×4=3
3	3×1=3	3×2= 1	3×3=4	3×4=2
4	4×1=4	4×2=3	4×3=2	4×4=1

Guardiamo inizialmente solo i risultati del prodotto: in ogni riga compaiono tutti gli elementi; se moltiplichiamo tra loro tutti i risultati nella stessa riga, il loro prodotto non dipende quindi dalla riga:

×	1	2	3	4	prodotto dei risultati
1	1	2	3	4	1×2×3×4 = 4
2	2	4	1	3	2×4×1×3= 4
3	3	1	4	2	3×1×4×2=4
4	4	3	2	1	4×3×2×1=4

Ora riscriviamo la moltiplicazione dei prodotti sulla stessa riga, raccogliendo le potenze come segue:

×	**1**	**2**	**3**	**4**	prodotto
1	1×1	1×2	1×3	1×4	$(1\times1)\times(1\times2)\times(1\times3)\times(1\times4) = 1^4 \times (1\times2\times3\times4) = 4$
2	2×1	2×2	2×3	2×4	$(2\times1)\times(2\times2)\times(2\times3)\times(2\times4) = 2^4 \times (1\times2\times3\times4)$
3	3×1	3×2	3×3	3×4	$(3\times1)\times(3\times2)\times(3\times3)\times(3\times4) = 3^4 \times (1\times2\times3\times4)$
4	4×1	4×2	4×3	4×4	$(4\times1)\times(4\times2)\times(4\times3)\times(4\times4) = 4^4 \times (1\times2\times3\times4)$

Uguagliando i risultati ottenuti, concludiamo che $4 = 2^4 \times 4 = 3^4 \times 4 = 4^4 \times 4$ cioè

$$1 = 2^4 = 3^4 = 4^4$$

In analogia a quanto visto, mostriamo che, quando *n* è primo, gli esponenti che possiamo utilizzare sono solo un numero finito (limitato da *n*) (dunque, le chiavi di cifratura sono in numero limitato):

Piccolo teorema di Fermat: *Se p è un numero primo e a non è divisibile per p, allora*

$$a^{p-1} = 1 \mod p.$$

Dimostrazione. L'elemento *a* è invertibile modulo *p* e quindi la moltiplicazione per [*a*] modulo *p* è iniettiva e manda [0] in [0]. L'insieme formato dagli elementi

$$\{[a], [2a], \ldots, [(p-1)a]\}$$

coincide quindi con l'insieme $\{[1], [2], \ldots, [p-1]\}$.
Il prodotto degli elementi del primo insieme deve pertanto essere uguale al prodotto di quelli del secondo:

$$[a^{p-1}]\,[2\times 3\times \ldots\times (p-2)\times (p-1)] = [2\times 3\times \ldots\times (p-2)\times (p-1)]$$

Poiché il prodotto $[2\times 3\times \ldots\times (p-2)\times (p-1)]$ è invertibile, otteniamo la tesi. ◊

Corollario *Le potenze si ripetono quindi in modo periodico, con periodo p-1:*
$a^k = a^{k+p-1} \mod p$ *e* $a^p = a \mod p$ *per ogni intero a.*

Possiamo utilizzare il Piccolo teorema di Fermat per individuare un metodo di cifratura: se per caso $h(p-1)+1 = e\,d$, allora $a^{ed} = a^{h(p-1)+1} = (a^{(p-1)})^h\ a = a \bmod n$.
Ma $a^{ed} = (a^e)^d$: dunque possiamo usare $m \to m^e$ per cifrare e $c \to c^d$ per decifrare.
Illustriamo il metodo con un esempio.

Esempio di cifratura e decifratura tramite Piccolo teorema di Fermat. Utilizziamo la seguente tabella di corrispondenza alfabeto-numeri modulo 11:

a	b	i	o	q	s	t	u	v
2	3	4	5	6	7	8	9	10

La funzione cifrante è f: $\mathbf{Z}_{11} \to \mathbf{Z}_{11}$ definita da $f(m) = m^3$, per ogni $m \in \mathbf{Z}_{11}$.
Il messaggio da cifrare è *stai qui.* Aiutandoci con la tavola della moltiplicazione (nella quale è stata eliminata la parte relativa a [0])

×	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

x	x^2	x^3
1	1	1
2	4	8
3	9	5
4	5	9
5	3	4
6	3	7
7	5	2
8	9	6
9	4	3
10	1	10

applichiamo la funzione di cifratura e otteniamo

s	t	a	i		q	u	i
$7^3 = 2$	$8^3 = 2$	$2^3 = 8$	$4^3 = 9$		$6^3 = 7$	$9^3 = 3$	$4^3 = 9$

Ora vediamo come procedere per decifrare un messaggio. Supponiamo di aver ricevuto il seguente messaggio, cifrato tramite la funzione di cifratura f: $\mathbf{Z}_{11} \to \mathbf{Z}_{11}$ definita da $f(m) = m^3$ a partire dalla medesima tavola alfabeto-numeri utilizzata sopra:

10 8 9 10 9 8 2 3 5 9 6 4

Per decifrare, serve la funzione inversa di f : la possiamo ricostruire leggendo da destra a sinistra la tabella in cui è calcolato il valore di x^3 a partire dal valore di x.
In alternativa, possiamo utilizzare il piccolo teorema di Fermat per descrivere la funzione inversa come un ulteriore elevamento a potenza: sappiamo infatti che in $\mathbf{Z}_{11}$ si ha $m^{11} = m$, $m^{k+10} = m^k$, cioè gli esponenti lavorano modulo 10. Sappiamo poi che MCD(3,10) = 1 e possiamo ricavare facilmente l'identità di Bézout $1 = 10 + (-3) \times 3$ che ci assicura che l'esponente $(-3) \times 3$ fornisce (modulo 11) gli stessi risultati dell'esponente 1. Ma, 7 è congruo a –3 modulo 10, e dunque

$$(m^3)^7 = m^{3\times 7} = m \quad \text{modulo } 11$$

e l'applicazione g: $\mathbf{Z}_{11} \to \mathbf{Z}_{11}$ definita da $g(c) = c^7$ è la funzione per decifrare.

c	10	8	9	10	9	8	2	3	5	9	6	4
$c^7=m$	10	2	4	10	4	2	7	9	3	4	8	5
messaggio in chiaro	v	a	i	v	i	a	s	u	b	i	t	o

x	x^2	x^3	x^6	x^7
1	1	1	1	1
2	4	8	9	7
3	9	5	3	9
4	5	9	4	5
5	3	4	5	3
6	3	7	5	8
7	5	2	4	6
8	9	6	3	2
9	4	3	9	4
10	1	10	1	10

La possibilità di esprime la funzione decifrante come potenza rispetto ad un esponente calcolabile a partire dal numero primo n e dall'esponente utilizzato per la cifratura è utile quando n è grande. Questo metodo non viene però normalmente utilizzato per cifrare, perché una sua variante (con n prodotto di due primi distinti) è molto più sicura.

Quando *n* è prodotto di due primi distinti: Teorema di Eulero
Se *n* non è primo?
Esempio Modulo 10:

	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\mathbf{x^2}$	**4**	**9**	**6**	**5**	**6**	**9**	**4**	**1**
$\mathbf{x^3}$	**8**	**7**	**4**	**5**	**6**	**4**	**2**	**9**
$\mathbf{x^4}$	**6**	**1**	**6**	**5**	**6**	**1**	**6**	**1**
$\mathbf{x^5}$	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Teorema di Eulero: *Se n= pq è prodotto di due numeri primi distinti e MCD(a,n)=1, allora*

$$a^{(p-1)(q-1)} = 1 \mod n.$$

Dimostrazione: Poichè MCD(a,n)=1, sappiamo che MCD(a,p)=1 *e* MCD(a,q)=1. Per il Piccolo Teorema di Fermat per il primo p, sappiamo che

$$a^{(p-1)} = 1 \mod p \text{ e dunque } a^{(p-1)(q-1)} = 1 \mod p.$$

Analogamente, per il Piccolo Teorema di Fermat per il primo q, sappiamo che

$$a^{(q-1)} = 1 \mod q \text{ e dunque } a^{(p-1)(q-1)} = 1 \mod q.$$

Sappiamo, quindi, che sia p che q dividono il numero $a^{(p-1)(q-1)} - 1$: poichè p e q sono primi distinti, concludiamo che anche il loro prodotto n divide tale numero, e abbiamo la tesi. ◊

Corollario 1: *Se $n = pq$ prodotto di due numeri primi distinti, allora*

$$a^{(p-1)(q-1)+1} = a \mod n.$$

1noltre, per ogni intero k,

$$a^{k\,(p-1)(q-1)+1} = a \mod n$$

***Dimostrazione*:** Se *MCD(a,n)=1,* basta utilizzare il Teorema.
Ora consideriamo $a = p$. Sicuramente $p^{(p-1)(q-1)+1} = p \mod p$ e

$$p^{k\,(p-1)(q-1)+1} = p \mod p \text{ per ogni } k.$$

Inoltre, poichè *MCD(p,q)=1,* osserviamo che $p^{(q-1)} = 1 \mod q$ per il Piccolo Teorema di Fermat, e quindi $(p^{(q-1)})^{k(p-1)} = 1 \mod q$; dunque

$$p^{k\,(q-1)\,(p-1)+1} = p \mod q \text{ per ogni } k;$$

poiché $p^{k\,(q-1)\,(p-1)+1} - p$ è divisibile sia per p che per q (che sono primi tra loro), tale numero è divisibile anche per $n = pq$ e il corollario è vero per $a = p$. Ma allora il corollario è vero anche per ogni potenza di p.
Se *MCD(a,n)=d ≠1,* possiamo supporre $d=p$ a meno di scambio dei nomi: infatti, se n divide a, la tesi è sicuramente vera. Altrimenti $a=p^m\ r$, ove r è un opportuno numero intero con *MCD(r,n) =1;* dunque

$$r^{k\,(p-1)\,(q-1)+1} = r \mod n$$

in base al Teorema, mentre $= p^{m\,[k\,(p-1)\,(q-1)+1]} = p^m \mod n$ per quanto appena osservato. Risulta $a^{k\,(p-1)\,(q-1)+1} = p^{m[k(p-1)\,(q-1)+1]}\ r^{k(p-1)\,(q-1)+1} = p^m\ r = a \mod n.$ ◊

Abbiamo imparato che alcuni esponenti non possono essere utilizzati per cifrare. Ma abbiamo imparato qualcosa di più: sappiamo scegliere alcuni esponenti giusti, e per essi sappiamo scrivere la funzione di decifratura:

Osservazione: se per caso $(p-1)(q-1)+1 = e\,d$, allora $a^{ed} = a^{(p-1)(q-1)+1} = a \mod n$.
Ma $a^{ed} = (a^e)^d$

Posso usare l'elevamento alla potenza con esponente *e* per cifrare e l'elevamento alla potenza con esponente *d* per decifrare.
Per ovviare il problema del numero limitato di chiavi e, contemporaneamente, non utilizzare sostituzioni monoalfabetiche, utilizziamo la cifratura a blocchi.

Possiamo rileggere in un altro modo la relazione tra *e* e *d*:

$$(p-1)(q-1)+1 = e\,d,$$

significa

$$(p-1)(q-1) = e\,d - 1,$$

dunque

$$e\,d = 1 \text{ modulo } (p-1)(q-1)$$

Le classi *e*, *d* sono inverse tra loro modulo $(p-1)(q-1)$

SISTEMI A CHIAVE PUBBLICA

Finora abbiamo descritto dei metodi di cifratura che fanno uso di una chiave privata, cioè di una informazione grazie alla quale si può sia criptare il messaggio che decifrarlo: tale chiave deve essere necessariamente nota sia al mittente che al destinatario. Mittente e destinatario sono a conoscenza della stessa informazione.

Immaginiamo ora che il destinatario voglia comunicare privatamente con più di una persona, anzi che voglia addirittura che chiunque sia in grado di inviargli messaggi cifrati, mantenendo però la segretezza di ciascuno. Con i sistemi a chiave privata, ciò non sarebbe possibile: il destinatario è in grado di ricevere messaggi solo da persone note, con le quali ha condiviso la chiave.

E' necessario quindi un sistema diverso, un metodo che preveda due informazioni indipendenti: una per cifrare e un'altra per decifrare; l'informazione per cifrare può allora essere resa nota a tutti (e viene chiamata *chiave pubblica*), mentre l'informazione che serve per decifrare (la *chiave privata*) va tenuta rigorosamente segreta: la conosce solo il destinatario e permette a lui soltanto di leggere i messaggi.
L'idea di utilizzare un sistema a doppia chiave è dovuta a Diffie e Hellman. Nel 1976, Diffie e Hellmann mettono le basi per un sistema crittografico in cui **la chiave per cifrare non permetta di ricavare la chiave per decifrare**: in tal modo è possibile (ad esempio per una banca) rendere pubblica la chiave per cifrare, permettendo a tutti di scrivere alla banca stessa in segretezza. Solo la banca è in grado di leggere il contenuto del messaggio, perchè possiede la chiave per decifrare.
La prima realizzazione pratica (per quanto noto) è dovuta a Rivest, Shamir e Adleman del MIT (Massachusetts Institute of Tecnology) e in loro onore prende il nome di *sistema RSA:* è attualmente il sistema più diffuso di crittazione.
I sistemi a chiave privata sono detti anche *simmetrici,* mentre quelli a chiave privata *asimmetrici*, perchè mittente e destinatario hanno, nel secondo caso, ruoli decisamente differenti.

Se B vuole che chiunque sia in grado di scrivergli, ha bisogno di rendere pubbliche tutte le informazioni necessarie per cifrare, facendo in modo che da tali informazioni non sia possibile risalire alle informazioni necessarie per decifrare. Occorre a tal fine che la chiave per decifrare non siano ottenibili (in modo facile) dalla chiave che serve per cifrare.

Ci è permesso, in tal modo, divulgare sia la chiave di cifratura che il metodo, ma senza per questo rivelare contestualmente il modo di decifrare. Il metodo di cifratura deve essere una funzione matematica abbastanza semplice che tutti sono in grado di utilizzare, mentre la funzione di decifratura deve poter essere applicata agevolmente solo da chi è in possesso della "chiave privata". Il tutto è quindi basato su una funzione cifrante, la cui inversa è complessa solo apparentemente e diventa improvvisamente molto semplice non appena la si guarda attraverso l'informazione aggiuntiva (data dalla chiave).

Scopriremo più avanti di quale funzione stiamo parlando e capiremo nelle prossime lezioni quale dato riveste il ruolo della chiave e perché questa informazione sia (almeno ad oggi) indispensabile.

Tuttavia, per quanto la funzione sia semplice concettualmente, la cifratura e la decifratura richiedono conti abbastanza complessi e non molto agevoli da trattare se non si usa il metodo migliore: ci imbatteremo, infatti, nel calcolo di congruenze in cui compaiono potenze con basi ed esponenti elevati.

E' vero che, solitamente, questi conti vengono svolti dai calcolatori (anche perché i numeri coinvolti sono costituiti da tantissime cifre e quindi non sono assolutamente trattabili a mano), ma cerchiamo comunque di capire (usando ovviamente cifre più piccole) come il computer lavora per calcolare queste potenze.

Per realizzare questo metodo useremo le potenze, il teorema di Eulero, la scrittura in blocchi.

RSA

La azienda RSA ha brevettato il sistema crittografico a chiave pubblica attualmente più diffuso. Il metodo è universalmente noto.
La RSA vende chiavi "certificate" che permettono di usarlo in sicurezza. Le chiavi vengono costruite a partire da coppie di numeri primi molto grandi.

Siamo capaci di trovare nuovi numeri primi grandi, ma non siamo capaci di fattorizzare in modo efficiente

Cifratura

Per usufruire del sistema è necessario procurarsi una chiave pubblica da iscrivere in un elenco di dominio pubblico, al quale potrà attingere chiunque voglia scriverci.
La chiave è costituita da due numeri, che indicheremo con n ed e, che possiamo scegliere come vogliamo purché n sia prodotto di due numeri primi molto grandi p e q ed e sia un qualsiasi numero relativamente primo con $p-1$ e $q-1$ e diverso da p e q (le motivazioni di questa richiesta ci saranno chiare in seguito).

Il destinatario, che chiameremo per comodità B, deve pubblicare la sua chiave (n,e): l'unica accortezza che B deve avere è di tenere nascosti i primi p e q che, come vedremo, saranno la sua chiave privata per decifrare.

Vediamo, col supporto di un esempio, come deve procedere il mittente A se vuole inviare un messaggio a B.

ESEMPIO **Chiave pubblica: (1003, 3)**
Chiave privata: ?
Voglio scrivere "vieni qui"
Trascrivo in cifre: 21 08 04 13 08 16 20 08
Divido in blocchi più piccoli di 1003:
210 804 130 816 200 823
(ho aggiunto, in fondo, una x=23)
I blocchi sono:
m_1=210 m_2=804 m_3=130 m_4=816 m_5=200 m_6=823
Cifro ogni blocco, facendone la potenza di indice e:
$c_1 = m_1^{\,e}$ modulo n cioè $(210)^3$ modulo 1003 : c_1=301
$c_2 = (804)^3$ modulo 1003: dunque c_2= 975
$c_3 = (130)^3$ modulo 1003: dunque c_3=430
$c_4 = (816)^3$ modulo 1003: dunque c_4=357
$c_5 = (200)^3$ modulo 1003: dunque c_5= 72
$c_6 = (823)^3$ modulo 1003: dunque c_6=445

Decifratura

Il destinatario conosce i fattori p e q di n. Calcola la sua chiave privata, che è il numero d tale che

$ed–1$ sia divisibile per $(p–1)(q–1)$

cioè

d è l'inverso di e mod $(p–1)(q–1)$.

ESEMPI di chiavi:

Chiave pubblica ($n = 21$, $e = 5$),

n è prodotto di due primi p $=3$ e $q = 7$

$(p–1)(q–1)= 2 \times 6 = 12$: *non ha fattori in comune con 5*

Chiave privata: cerco un numero d tale che $5\ d–1$ sia divisibile per $(p–1)(q–1) =12$. *Ho bisogno che* $5\ d = 1+12$ *h: osservo che*

$5\times 5=25 = 1+24= 1+2\times12$: *dunque d =5 va bene :* ***ma è uguale alla chiave pubblica.....***

Chiave pubblica ($n = 21$, $e = 17$),

n è prodotto di due primi p $=3$ e $q = 7$

$(p-1)(q-1)= 2 \times 6 = 12$: *non ha fattori in comune con 17*

Chiave privata: cerco un numero d tale che $17d–1$ sia divisibile per $(p-1)(q-1) =12$. *Ho bisogno che* $17\ d = 1+ 12$ *h: osservo che*

$17\times5=85 = 1+84 = 1+7\times12$: *dunque d =5 va bene*

[il prodotto *ed* coincide con 1 sull'orologio con 21 ore]

(se siete preoccupati perchè avevamo appena detto che l'inverso di 5 mod 12 è proprio 5, basta osservare che 5 e 17 danno la stessa classe mod 12]

Il destinatario sa che 1003 = 17 x 59 (chiamo $p = 17$, $q = 59$) Deve **calcolare la chiave privata *d*** tale che $ed–1$ sia divisibile per $(p–1)(q–1)= 16\times58 = 928$. Ricava **d=619**.

Decifra ogni blocco, iniziando dal primo: **la procedura è uguale a quella della cifratura, ma l'esponente da usare è la chiave segreta**

$m_1= c_1{}^d$ modulo n cioè $(301)^{619}$ modulo 1003: $\boldsymbol{m_1=210}$

$m_2= (975)^{619}$ modulo 1003: dunque $\boldsymbol{m_2= 804}$

$m_3= (430)^{619}$ modulo 1003: dunque $\boldsymbol{m_3= 130}$

$m_4= (357)^{619}$ modulo 1003: dunque $\boldsymbol{m_4= 816}$

$m_5= (72)^{619}$ modulo 1003: dunque $\boldsymbol{m_5= 200}$

$m_6= (445)^{619}$ modulo 1003: dunque $\boldsymbol{m_6= 823}$

Ma perché questo procedimento ha funzionato? E' facile dimostrarlo sfruttando i risultati che abbiamo imparato sulle congruenze: (prendiamo $m = m_i$)

$$c^d = (m^e)^d = m^{e\ d} \text{ mod } (n)$$

Ma d'altra parte $ed = 1$ mod $(p-1)(q-1)$ e quindi, per definizione di congruenza, $ed – 1$ è un multiplo di $(p-1)(q-1)$, cioè

$$ed = 1+ k\ (p-1)(q-1) \qquad \textit{per un certo } k$$

Quindi

$$m^{ed} = m^{1\ +\ k\ (p-1)(q-1)} = m \times m^{\,k\ (p-1)(q-1)} = m \times (m^{\,(p-1)(q-1)})^k$$

Per il teorema di Eulero $m^{k\,(p-1)(q-1)} = m \mod (n)$
e quindi

$$m^{e\,d} = m \mod (n)$$

Osserviamo, infine, che quando il mittente ha cifrato il messaggio abbiamo richiesto che ciascun blocco di numeri m_i fosse minore di n: questo per garantire che non ci fosse ambiguità in fase di decrifratura nella determinazione del numero congruo a c^d modulo n.
Quest'ultimo è, infatti, l'unico numero che soddisfa la congruenza compreso tra 0 e $n-1$.

Ricostruiamo, per finire, tutto il viaggio da A a B del nostro messaggio in una tabella: