Sia n un numero naturale (non nullo e, in generale, maggiore di 1). Due numeri interi che hanno lo stesso resto nella divisione per n si dicono *congruenti modulo* n (o mod n) ; se due numeri $a, b \in \mathbf{Z}$ 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 intero a è congruente mod n al suo resto nella divisione per n, cioè all'unico naturale numero 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 $0, \ldots, n-1$. Per poter verificare in modo diretto se due numeri sono congruenti modulo n, senza bisogno di calcolare esplicitamente i resti della divisione per n, riformuliamo la precedente definizione come segue:

Definizione Sia n un intero positivo fissato. Due numeri $a, b \in \mathbf{Z}$ sono congruenti modulo n se $a - b$ è un multiplo di n, ovvero, $a \equiv b \bmod n \Leftrightarrow (a-b) = n \cdot h$ per qualche $h \in \mathbf{Z}$.

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

Osservazioni Chiamiamo *congruenza* la relazione definita sugli interi dall'essere congruenti. Essa è una relazione di equivalenza. Infatti:
1) Ogni numero è congruente a se stesso, modulo qualsiasi naturale n: dunque per la congruenza vale la proprietà riflessiva.
2) $a \equiv b \bmod n$ se e solo se $(a-b) = n \cdot h$, cioè $(b-a) = n \cdot (-h)$ e dunque $b \equiv a$: dunque per la congruenza vale la proprietà simmetrica.
3) Se $a \equiv b \bmod n$ e $b \equiv c \bmod n$, allora $(a-b) = n \cdot h$ e $(b-c) = n \cdot k$, e dunque $(a-c) = (a-b+b-c) = (a-b) + (b-c) = n \cdot h + n \cdot k = n \cdot (h+k)$ e dunque $a \equiv c \bmod n$. Dunque per la congruenza vale la proprietà transitiva.

La congruenza modulo n è quindi una relazione di equivalenza. La congruenza divide quindi gli interi in sottoinsiemi tra loro disgiunti:

Definizione Dato $a \in \mathbf{Z}$, si denota con $\overline{a}$ oppure con $[a]$ l'insieme

$$\overline{a} = \{b \in \mathbf{Z} \text{ tale che } b \equiv a \bmod n\}.$$

detto *classe resto* di a modulo n. Si dice che a rappresenta (o è rappresentante di) tale insieme. A volte, per semplicità, si scrive semplicemente a per denotare sia il numero che la sua classe (quando il contesto chiarisce il significato da applicare).

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 $0, \ldots, n-1$. Dunque le classi resto modulo n sono esattamente n e ciascuna di esse ha uno ed un solo rappresentante in $\{0, 1, 2, ..., n-1\}$. Spesso useremo il rappresentante della classe scelto con questo criterio.

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

Esempio a) Le classi resto modulo 4 sono: $\overline{0} = \{$ interi che divisi per 4 danno resto 0$\}$
$\overline{1} = \{$ interi che divisi per 4 danno resto 1$\}$
$\overline{2} = \{$ interi che divisi per 4 danno resto 2 $\}$
$\overline{3} = \{$ interi che divisi per 4 danno resto 3 $\}$.
b) Per studiare la classe di congruenzamodulo n, possiamo modificare il rappresentante sommando o sottraendo multipli di n: [67] mod 6 = [7] mod 6.

Definizione Si definiscono due operazioni in $\mathbf{Z}_n$. Date due classi resto $[a]$ e $[b]$ modulo n, si pone:

la somma di classi resto $[a] + [b] = [a + b]$

il prodotto di classi resto $[a] \cdot [b] = [a \cdot b]$

Osserviamo che la definizione di queste operazioni è ben posta, cioè è indipendente dalla scelta del rappresentante della classe. Ad esempio, possiamo mostrare che la somma è ben definita: 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. Ad esempio: $[18] + [21] = [3]$ mod 4 : infatti $18 + 21 = 39$ e $[39] = [3]$ mod 4 perch $39 = 4 \cdot 9 + 3$. 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: ad esempio, $[17] \cdot [10] = [170] = [2]$ mod 6. D'altronde [17]=[5] mod 6 e [10]=[4] mod 6: potevo dunque scrivere $[5] \cdot [4] = [20] = [2]$ mod 6.

Si noti che somma e prodotto godono delle proprietà associativa e commutativa, oltre che delle proprietà distributiva della somma rispetto al prodotto (perché?). Inoltre

$[a]$ +[0] = $[a]$ per ogni a e dunque la classe [0] svolge il ruolo dello 0 negli interi;

$[a]$ +$[-a]$ = [0] per ogni a e dunque la classe $[-a]$ svolge il ruolo della classe opposto.

Esercizi

1.1) 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 : .....

-3 modulo 6 : .....

74 modulo 23 : .....

-7 modulo 5 : .....

1.2) Stabilisci se le seguenti congruenze sono verificate:

V F $16 \equiv 31$ mod 5

V F $25 \equiv 13$ mod 13

V F $72 \equiv -21$mod 31

V F $82 \equiv 59$ mod 29

1.3) Siano $a, b, n \in \mathbf{Z}$, con $n > 0$. Mostra che $a \equiv b \pmod{n}$ se e solo se il resto della divisione di a per n è uguale al resto della divisione di b per n.

1.4) Mettere in evidenza il rappresentante tra 0 e 7 e ripartire in classi uguali mod 8: [16], [47], [54], [67], [76], [116], [89].

1.5) $a, b, c, d, n, m \in \mathbf{Z}$, $n, m > 0$,

a) Prova che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ allora $ac \equiv bd \pmod{n}$.

b) Prova che $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$ se e solo se $a \equiv b \pmod{mcm(n, m)}$

1.6) Prova che, se $n|$ e m sono numeri naturali, con $n[m$, allora $\varphi : \mathbf{Z}_m \to \mathbf{Z}_n$, $[a]_m \mapsto [a]_n$ è ben definita ed è suriettiva. Scrivi esplicitamente questa applicazione quando $m = 6, n = 3$.

Tratteremo le classi modulo n come elementi di $\mathbf{Z}_n$ (mantenendo sia la parola classe, che la parola elemento).

Non bisogna pensare che tutte le proprietà con cui siamo soliti lavorare in $\mathbf{Z}$ restino valide in $\mathbf{Z}_n$. Ad esempio la legge di cancellazione (se $[a]$ è non nullo e $[a] \cdot [b] = [a] \cdot [c]$, allora $[b] = [c]$) che vale in $\mathbf{Z}$ non si trasporta alle congruenze; ad esempio: $[2] \cdot [2] = [2] \cdot [6]$ mod 8 ma $[2] \neq [4]$ mod 8.
In particolare, l'applicazione $\mathbf{Z}_8 \to \mathbf{Z}_8$, $[a] \mapsto [2] \cdot [a]$ non è iniettiva.

Osserviamo un'altra particolarità: in $\mathbf{Z}_6$, si ha che [2] e [3] sono entrambe non nulli (cioè diversi dalla classe nulla [0]), ma il loro prodotto è la classe nulla: $[2] \cdot [3] = [0]$. Introduciamo la definizione:

Definizione Un elemento non nullo $[a]$ di $\mathbf{Z}_n$ è un *divisore di zero* (o, divisore dello zero) se esiste un elemento non nullo $[b]$ tale che $[a] \cdot [b] = [0]$.

Osserviamo che se $n = p \cdot q$ con $1 < p, q < n$, allora le classi $[p]$ e $[q]$ sono divisori di zero: infatti, $[p] \cdot [q] = [0]$ ma né p né q sono nulli. Inoltre, $[p] \cdot [q] = [0] = [p] \cdot [0] = [0] \cdot [q]$: dunque la moltiplicazione per $[p]$ e la moltiplicazione per $[q]$ non definiscono una applicazione iniettiva in tal caso (e la legge di cancellazione non vale per fattori che sono divisori di zero).

Possiamo dimostrare un risultato più generale:

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

$$\begin{array}{ccc} \mathbf{Z}_n & \to & \mathbf{Z}_n \\ [m] & \mapsto & [a] \cdot [m] \end{array} \tag{1}$$

Dimostrazione Osserviamo che la moltiplicazione (1) è iniettiva se e solo se è biettiva. Dunque, basta controllare l'iniettività. Supponiamo che MCD(a,n) =1 e mostriamo che la moltiplicazione (1) è iniettiva. Per ipotesi, n non divide a, e la classe $[a]$ è non nulla in $\mathbf{Z}_n$. Prendiamo due numeri h e k con h e k 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 $ak - ah = tn$, allora sarebbe anche $a(k - h) = tn$; ma, poichè MCD(a, n) =1 , il numero n deve dividere $(k - h)$: ma questo è impossibile, perch $(h - k)$ è in valore assoluto minore di n.

Supponiamo ora che la moltiplicazione (1) 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 $n = dk$, $a = dh$ per opportuni interi $0 < h$, $k < n$. Ma allora, [0] e $[k]$ hanno la stessa immagine nella moltiplicazione (1): infatti

$$[a] \cdot [k] = [ak] = [(dh)k] = [(hd)k] = [h(dk)] = [hn] = [0] = [a] \cdot [0]$$

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

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

Cerchiamo di comprendere questo risultato da un altro punto di vista. Supponiamo che la moltiplicazione per $[a]$ 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 $[m] \in \mathbf{Z}_n$ tale che $[a] \cdot [m] = [1]$.
Definizione Una classe$[a] \in \mathbf{Z}_n$ si dice *invertibile* se esiste $[m]$ in $\mathbf{Z}_n$ tale che $[a] \cdot [m] = [1]$. Una tale classe $[m]$ è chiamata *inversa* di $[a]$ in $\mathbf{Z}_n$ e viene indicata con il simbolo $[a]^{-1}$.

Osserviamo che, in tal caso, $[a] \cdot [a]^{-1} = [a]^{-1} \cdot [a] = [1]$.
Proposizione 2 Una classe $[a]$ è invertibile in $\mathbf{Z}_n$ se e solo se $MCD(a, n) = 1$, cioè se e solo se risulta biettiva la moltiplicazione (1) $\mathbf{Z}_n \to \mathbf{Z}_n$, $[m] \mapsto [a] \cdot [m]$ In tal caso, l'applicazione inversa di (1) è la

moltiplicazione per l'inverso $[a]^{-1}$ di $[a]$:

$$\begin{array}{ccc} \mathbf{Z}_n & \to & \mathbf{Z}_n \\ [c] & \mapsto & [a]^{-1} \cdot [c] \end{array} \tag{2}$$

Dimostrazione Abbiamo visto che l'invertibilità di $[a]$ è una condizione necessaria affinchè la moltiplicazione sia biettiva. Tale condizione risulta essere anche sufficiente. Basta provare che, se $[a]$ è invertibile, allora (2) è la funzione inversa di (1), provando a comporre queste due funzioni.

$$[m] \mapsto [a] \cdot [m] \mapsto [a]^{-1}([a] \cdot [m]) = [a]^{-1} \cdot [a] \cdot [m] = [m]$$

$$[c] \mapsto [a]^{-1} \cdot [c] \mapsto [a] \cdot ([a]^{-1} \cdot [c]) = (a \cdot [a]^{-1}) \cdot [c] = [c]$$

Poichè entrambe le composizioni sono lidentità, la funzione (1) è invertibile, e (2) è la sua inversa.

Come esercizio, dimostriamo direttamente che se $[a]$ è invertibile, l'applicazione (1) è suriettiva; infatti, comunque scelto $[c]$ in $\mathbf{Z}_n$, si può scrivere $[c] = [1] \cdot [c] = ([a] \cdot [a]^{-1}) \cdot [c] = \overline{a} \cdot ([a]^{-1} \cdot [c])$; dunque lelemento $\overline{q}$ è immagine dell'elemento $[m] = [a]^{-1}[c]$, tramite l'applicazione (1): ogni elemento del codominio appartiene all'immagine della moltiplicazione (1).

Se avessimo voluto provare in modo diretto l'iniettività di (1), potevamo procedere come segue: supponiamo che le classi $[m]$ e $[m]'$ abbiano la stessa immagine, cioè $[a] \cdot [m] = [a] \cdot [m]'$. Si ricava: $[m] = [1] \cdot [m] = ([a]^{-1} \cdot [a]) \cdot [m] = [a]^{-1} \cdot ([a] \cdot [m]) = [a]^{-1} \cdot ([a] \cdot [m]') = ([a]^{-1} \cdot [a]) \cdot [m]' = [1] \cdot [m]' = [m]'$, da cui l'iniettività di (1).

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

Corollario 2 Se p è primo, ogni elemento non nullo $[a]$ di $\mathbf{Z}_p$ è invertibile in $\mathbf{Z}_p \setminus \{[0]\}$.

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

Se MCD(a,n)=1, allora, in base alla relazione di Bézout, esistono interi s e t tali che $1 = s \cdot a + t \cdot n$. Prendendo le classi modulo n, scopriamo che $[1] = [s] \cdot [a] + [t] \cdot [n] = [s] \cdot [a] + [t] \cdot [0] = [s] \cdot [a]$ Dunque $[a]$ è invertibile, e $[s]$ è il suo inverso.

Esercizi

2.1) Completa la tavola additiva e la tavola moltiplicativa in $\mathbf{Z}_6$ e in $\mathbf{Z}_7$.

2.2) $a, b, c, n \in \mathbf{Z}$, $n > 0$. Prova che se $ac \equiv bc \pmod{n}$ e $MCD(c, n) = 1$, allora $a \equiv b \pmod{n}$.

2.3) MCD(5363, 3277) = ... L'inverso di 3277 mod 5363 è .....

2.4) MCD(71021, 3277)= ..... Discuti la risolubiltà di $[3277]x \equiv [2]$ in $\mathbf{Z}_{71021}$.

2.5) Calcola le soluzioni di $[6]x \equiv [9]$ in $\mathbf{Z}_5$ e in $\mathbf{Z}_{12}$.

Applicazioni alla crittografia

L'utilizzo delle classi di congruenza facilita l'implementazioni di vari sistemi crittografici. La cifratura è una operazione di passaggio da un insieme di messaggi (detti *messaggi in chiaro*) ad un altro insieme di messaggi (detti *messaggi cifrati*) il cui significato è nascosto: può dunque essere interpretata come una funzione tra questi due insiemi. È possibile cifrare singole parole (basta pensare ad un vocabolario inglese-italiano, ad esempio) o cifrare le singole lettere dell'alfabeto (o altre soluzioni intermedie).

Sistema di Cesare

Svetonio, 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 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 'fuoco', il messaggio cifrato sarà ' IARFR'.

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**. 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.

Più in generale, un crittosistema è costituito da una terna (P, K, C):

a) l'insieme dei messaggi in chiaro P i cui elementi vengono indicati spesso con la lettera m;

b) l'insieme delle chiavi K in cui ogni elemento k determina una trasformazione di cifratura e una trasformazione di decifratura che sono una l'inversa dell'altra;

c) l'insieme dei messaggi cifrati C i cui elementi sono indicati spesso con la lettera c.

Nel cifrario di Cesare:

a) gli elementi $m \in P$ sono le parole che vogliamo inviare (in una lingua fissata);

b) la chiave consiste in fase di cifratura nello spostare di tre posti le varie lettere e in fase di decifratura nel rimetterle nella loro corretta posizione;

c) 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 dellalfabeto: 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 dellalfabeto in chiaro corrispondano lettere diverse dell'alfabeto cifrante (perchè questo ci assicura che sia 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. Si noti che ogni funzione iniettiva di un insieme finito in se stesso, è automaticamente suriettiva (e quindi biettiva).

Per descrivere in modo più efficiente le funzioni di cifratura nel caso del cifrario di Cesare, assegniamo ad ogni lettera dell'alfabeto italiano in chiaro un numero corrispondente alla sua posizione come nella seguente tabella:

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Se la chiave cifrante è 5, l'operazione di cifratura consiste nel sommare 5 (modulo 21), in modo che le ultime lettere dell'alfabeto abbiano la giusta immagine. Per questo motivo, i cifrari di tipo Cesare sono detti anche cifrari per traslazione.

Il metodo di Cesare (e tutti i metodi basati sulla cifratura lettera a lettera fatta in modo tale che la stessa lettera venga sempre cifrata allo stesso modo) sono considerati insicuri, perchè sono attaccabili grazie all'**analisi delle frequenze**.

Sistemi a chiave pubblica Il metodo di Cesare è un metodo a chiave privata, cioè l'informazione grazie alla quale si può sia criptare permette facilmente anche di 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 per 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. 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 sia ottenibile (in modo facile) dalla chiave che serve per cifrare.

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).

Nel metodo RSA, la cifratura e la decifratura richiedono il calcolo di potenze modulo n con basi ed esponenti elevati) nel caso in cui $n = pq$ sia il prodotto di due primi distinti. Per impararne e giustificarne il funzionamento, approfondiamo lo studio delle proprietà degli elementi invertibili modulo n. Saremo interessati soprattutto ai casi in cui $n = p$ è primo oppure $n = p \times q$ è prodotto di due primi distinti.

Gruppo moltiplicativo degli invertibili

Denotiamo con $\mathbf{Z}_n^*$ il sottoinsieme di $\mathbf{Z}_n$ formato dagli elementi invertibili di $\mathbf{Z}_n$. Osserviamo che

a) $\mathbf{Z}_n^*$ è non vuoto perché contiene [1],

b) che il prodotto di due elementi invertibili è un elemento invertibile (diciamo che $\mathbf{Z}_n^*$ è chiuso rispetto alla moltiplicazione),

c) che l'inverso di un elemento invertibile è un elemento invertibile (diciamo che $\mathbf{Z}_n^*$ è chiuso rispetto all'inverso).

E' un esempio di una struttura più generale, detta *gruppo* (moltiplicativo commutativo). Queste struttura è alla base di alcune dimostrazioni.
Esempi: a) se p è un primo, $\mathbf{Z}_p^* = \{[1], [2], \ldots, [p-1]\}$.
b) se $n = p \times q$ è prodotto di due primi distinti, gli invertibili sono tutte le classi il cui rappresentante è coprimi sia con p che con q. A partire dagli $n-1$ rappresentanti tra 1 e $n-1$, basta eliminare i multipli di p e i multipli di q. I multipli non nulli di p sono p, $2p$, $3p$, ..., $(q-1)p$ (sono $q-1$). I multipli non nulli di q sono q, $2q$, $3q$, ..., $(p-1)q$ (sono $p-1$). Gli invertibili sono dunque $(n-1)-(q-1)-(p-1) = p \times q - 1 - q + 1 - p + 1 = p \times q - q - p + 1 = (p-1)(q-1)$.
c) per ogni n, gli invertibili sono tutte le classi (non nulle) che ammettono un rappresentante tra 1 e $n-1$ coprimo con n: il numero dei numeri naturali (non nulli) più piccoli di n e coprimi con n viene indicato con un simbolo:

$$\varphi(n).$$

Si interpreta φ come una funzione di variabile n, detta la funzione di Eulero.

Osservazione Se p è un primo, una classe invertibile $[a]$ coincide con il proprio inverso se $[a] = [a]^{-1}$, cioè se $[a]^2 = [1]$: quindi $[a]$ coincide con il proprio inverso se e solo se $[a]$ è soluzione (in $\mathbf{Z}_p$) dell'equazione $x^2 - [1] = [0]$. Ma $x^2 - [1] = (x - [1])(x + [1])$ e (poichè non ci sono divisori di 0 in $\mathbf{Z}_p$) questo prodotto si può annullare se e solo se uno dei due fattori si annulla. Ma se si annulla il primo fattore, allora $x = [1]$, mentre se si annulla il secondo allora $x = -[1]$. Dunque, in $\mathbf{Z}_p$, gli unici elementi che coincidono con il proprio inverso sono $[1]$ e $-[1]$.

Questa osservazione ci sarà utile per dimostrare il seguente:

Teorema di Wilson Se p è un numero primo, allora $(p-1)! \equiv -1 \bmod p$.
Dimostrazione. Si consideri il prodotto di tutti gli elementi invertibili in $\mathbf{Z}_p$. In questo prodotto, gli elementi diversi da $[1]$ e $-[1]$, si suddividono in coppie (un fattore e il proprio inverso): il prodotto di ciascuna di queste coppie è uguale a $[1]$. Svolti questi prodotti, restano solo i fattori $[1]$ e $-[1]$, e il risultato del prodotto è $-[1]$.

Anche a fini crittografici, studiamo le potenze di un elemento.

Piccolo teorema di Fermat a) Se p è un numero primo $[a] \in \mathbf{Z}_p$ è non nullo, allora $[a]^{p-1} = [1]$; dunque, $[a]^p = [a]$ per ogni $[a]$.
b) Se a non è divisibile per p, allora $a^{p-1} \equiv 1 \bmod p$. Dunque, $a^p \equiv a \bmod p$ per ogni a.
Dimostrazione 1: Osserviamo che *per ogni primo p e ogni $x, y \in \mathbf{Z}$, vale la seguente congruenza:*

$$(x+y)^p \equiv x^p + y^p \quad mod\, p$$

Infatti, $(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} x^k y^k + y^p$ e la sommatoria è divisibile per p, perché in essa k e $p-k$ sono minori di p e il numero $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ è un intero che ha p come fattore.
Mostriamo dunque l'enunciato del teorema. Supponiamo inizialmente che $a \geq 0$ e procediamo per induzione su a. Se $a = 0$, la tesi è vera. Supponiamo vera la tesi per a (cioè supponiamo che $a^p \equiv a \bmod p$) e mostriamo che esse è vera anche per $a+1$. Per quanto osservato, $(a+1)^p \equiv a^p + 1^p \equiv a^p + 1 \quad mod\, p$. Ma $a^p \equiv a \bmod p$ per ipotesi induttiva, quindi $(a+1)^p \equiv a+1$ e la tesi è vera.

Supponiamo ora $a \leq 0$ e osserviamo che $0 \equiv 0^p = (a + (-a))^p \equiv a^p + (-a)^p \bmod p$. Poiché $-a \geq 0$, per quanto appena dimostrato $(-a)^p \equiv -a$; concludiamo che $0 = a^p - a$, cioè $a^p \equiv a$.
Dimostrazione 2: sfruttiamo in modo più evidente la struttura di gruppo moltiplicativo. I due enunciati sono equivalenti, quindi basta dimostrare il primo. L'elemento $[a]$ è invertibile modulo p e quindi la moltiplicazione per a è iniettiva e manda 0 in 0. L'insieme formato dagli elementi

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

coincide quindi con

$$[1], [2], \ldots, [(p-1)].$$

Quindi il prodotto degli elementi del primo insieme deve essere uguale al prodotto di quelli del secondo:

$$[a] \cdot [2a] \cdot \ldots \cdot [(p-1)a] = [1] \cdot [2] \cdot \ldots \cdot [(p-1)].$$

Ma il prodotto a sinistra coincide con $[a]^{p-1} \cdot ([1] \cdot [2] \cdot \ldots \cdot [(p-1)])$. Poiché $([1] \cdot [2] \cdot \ldots \cdot [(p-1)])$ è invertibile, otteniamo la tesi.

Osservazione: nelle ipotesi del piccolo teorema di Fermat, poiché $[a]^{p-1} = [1]$ e $[a]^p = [a]$ per ogni $[a]$, valgono anche (per ogni $s > 0$)

a) $[a]^{p \cdot s} = [a]^s$.

b) Inoltre, $[a]^s = [a]^{p-1+s}$

E se n non è primo?

Teorema di Eulero Se $n = pq$ è prodotto di due numeri primi distinti e MCD(a, n)=1, allora $a^{(p-1)(q-1)} = 1 \bmod n$.

Dimostrazione: Poiché 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 $a^{(p-1)} = 1 \bmod p$ e dunque $a^{(p-1)(q-1)} = 1 \bmod p$. Analogamente, per il Piccolo Teorema di Fermat per il primo q, sappiamo che $a^{(q-1)} = 1 \bmod q$ e dunque $a^{(p-1)(q-1)} = 1 \bmod q$. Dunque sia p che q dividono il numero $a^{(p-1)(q-1)} - 1$: poiché p e q sono primi distinti, concludo che anche il loro prodotto n divide tale numero, e ho la tesi.

Esempio: Modulo 10:

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

Corollario 1 Se $n = pq$ è prodotto di due numeri primi distinti, allora $a^{(p-1)(q-1)+1} = a \bmod n$.

Dimostrazione: Se MCD(a, n)=1, basta utilizzare il Teorema. Ora consideriamo $a = p$: poiché MCD(p, q)=1, osservo che $p^{(q-1)} = 1 \bmod q$ per il Piccolo Teorema di Fermat, e quindi $(p^{(q-1)})^{(p-1)} = 1 \bmod q$ per il Piccolo Teorema di Fermat: dunque il corollario è vero per $a = p$. Ma allora il teorema è vero per ogni potenza di p.

Se MCD(a, n)=$d \neq 1$, posso supporre $d = p$ a meno di scambio dei nomi: infatti, se n divide a, la tesi è sicuramente vera. Allora $a = p^m r$, ove r è un opportuno numero intero con MCD(r, n) =1; dunque $r^{(p-1)(q-1)+1} = r \bmod n$ in base al Teorema, mentre $(p^m)^{[(p-1)(q-1)+1]} = p^m \bmod n$ per quanto appena osservato. Risulta che $a^{(p-1)(q-1)+1} = p^{m[(p-1)(q-1)+1]} r^{(p-1)(q-1)+1} = p^m r \bmod n$.

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

1) Calcola il prodotto di tutti gli elementi di $\mathbf{Z}_6$ e di tutti gli elementi di $\mathbf{Z}_7$.

2) n naturale. Prova che $7^n \equiv 1 \pmod 8$ se n è pari, $7^n \equiv 7 \pmod 8$ se n è dispari.

3) Calcola $[3]^{75}$ in $\mathbf{Z}_7$ e in $\mathbf{Z}_6$.