

1. Gruppi.

In questo paragrafo introduciamo i gruppi. Diamo diversi esempi importanti di gruppi ai quali faremo continuamente riferimento in seguito.

Definizione. Un gruppo G è un insieme fornito di una *operazione* $\circ : G \times G \longrightarrow G$ per cui valgono i seguenti assiomi:

(G_1) (*Associatività*) Per ogni $x, y, z \in G$

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

(G_2) (*Elemento neutro*) Esiste un elemento $e \in G$ tale che per ogni $x \in G$

$$x \circ e = e \circ x = x.$$

(G_3) (*Inverso*) Per ogni $x \in G$ esiste $x^* \in G$ tale che

$$x \circ x^* = x^* \circ x = e.$$

Se *in aggiunta* vale l'assioma

(G_4) (*Commutatività*) Per ogni $x, y \in G$

$$x \circ y = y \circ x.$$

il gruppo G si dice *commutativo* oppure *abeliano*.

Osservazione.

- (i) Non tutti i gruppi sono abeliani.
- (ii) Per l'associatività (G_1), le due espressioni $x \circ (y \circ z)$ ed $(x \circ y) \circ z$ sono uguali per ogni $x, y, z \in G$. Ecco perché possiamo omettere le parentesi e scrivere $x \circ y \circ z$.
- (iii) L'elemento neutro dell'assioma (G_2) è unico: infatti se ce ne fossero due e_1 ed e_2 , dall'assioma (G_2) avremmo

$$e_1 = e_1 \circ e_2 = e_2.$$

- (iv) L'elemento inverso x^* associato a $x \in G$ nell'assioma (G_3) è unico: se x^* e x^{**} soddisfano $x \circ x^* = x^* \circ x = e$ ed anche $x \circ x^{**} = x^{**} \circ x = e$ allora

$$x^* \stackrel{(G_2)}{=} e \circ x^* = (x^{**} \circ x) \circ x^* \stackrel{(G_1)}{=} x^{**} \circ (x \circ x^*) \stackrel{(G_3)}{=} x^{**} \circ e \stackrel{(G_2)}{=} x^{**},$$

cioè, $x^* = x^{**}$. Dunque ha senso chiamare x^* l'elemento inverso di x .

Esempio (1.1). I gruppi additivi \mathbf{Z} , \mathbf{Q} ed \mathbf{R} .

L'insieme \mathbf{Z} degli numeri interi è un gruppo rispetto all'addizione. È ben noto che valgono gli assiomi G_1 , G_2 e G_3 . L'elemento neutro è 0. L'inverso di un numero intero n è il suo *opposto* $-n$. Anche G_4 vale: \mathbf{Z} è un gruppo commutativo. Si verifica in modo simile che anche i numeri razionali \mathbf{Q} e i numeri reali \mathbf{R} formano un gruppo rispetto all'addizione. Anche in questi casi, l'elemento neutro è 0, l'inverso è l'opposto. I gruppi \mathbf{Q} ed \mathbf{R} sono anch'essi commutativi.

I numeri naturali $\mathbf{N} = \{1, 2, \dots\}$ invece non formano un gruppo per l'addizione. Ad esempio G_3 non vale: nell'insieme degli interi positivi non c'è inverso.

Esempio (1.2). I gruppi moltiplicativi \mathbf{Q}^* e \mathbf{R}^* .

Definiamo

$$\begin{aligned}\mathbf{Q}^* &= \mathbf{Q} - \{0\}, \\ \mathbf{R}^* &= \mathbf{R} - \{0\}.\end{aligned}$$

Siccome il prodotto ab di due numeri a, b non nulli è diverso da zero, l'assioma G_0 vale per \mathbf{Q}^* e \mathbf{R}^* ; vale a dire l'operazione $\mathbf{Q}^* \times \mathbf{Q}^* \rightarrow \mathbf{Q}^*$ data da $(a, b) \mapsto ab$ è ben definita e similmente per \mathbf{R}^* . Si verifica che valgono gli assiomi G_1, G_2, G_3 e G_4 : l'elemento neutro è 1, ogni $a \neq 0$ ha un inverso che è il suo *reciproco* $\frac{1}{a}$. Dunque \mathbf{Q}^* e \mathbf{R}^* sono gruppi commutativi rispetto alla moltiplicazione. Invece $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$ non è un gruppo per la moltiplicazione: due numeri interi si possono moltiplicare tra di loro, l'elemento neutro è 1, ma mancano gli inversi moltiplicativi. Per esempio, se $x \in \mathbf{Z}$ fosse l'inverso di 2, allora sarebbe $2x = 1$ e questa equazione non ha soluzioni in \mathbf{Z} .

Esempio (1.3). Il gruppo additivo dei numeri complessi \mathbf{C} .

L'insieme dei numeri complessi \mathbf{C} è definito come

$$\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$$

dove “ i ” denota $\sqrt{-1}$, e soddisfa $i^2 = -1$. Due numeri complessi $a + bi$ ed $a' + b'i$ sono uguali se e soltanto se $a = a'$ e $b = b'$. Se $b = 0$ si scrive spesso a per $a + bi = a + 0i$.

Addizioniamo due numeri complessi $a + bi$ ed $a' + b'i$ secondo la regola

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i.$$

Si verifica che in questo modo \mathbf{C} diventa un gruppo per l'addizione. L'elemento neutro è $0 = 0 + 0i$. L'inverso di un numero complesso $a + bi$ è il suo opposto $-a - bi$. L'insieme \mathbf{C} è detto il gruppo *additivo* dei numeri complessi.

Esempio (1.4). Il gruppo moltiplicativo dei numeri complessi \mathbf{C}^* .

Moltiplichiamo due numeri complessi $a + bi$ e $a' + b'i$ secondo la regola

$$(a + bi) \cdot (a' + b'i) = (aa' - bb') + (ab' + a'b)i.$$

La regola per la moltiplicazione si ottiene sviluppando il prodotto $(a + bi) \cdot (a' + b'i)$ e tenendo conto che $i^2 = -1$. Si vede facilmente che $1 \in \mathbf{C}$ ha la proprietà $1 \cdot (a + bi) = (a + bi) \cdot 1 = a + bi$, ossia è l'elemento neutro per la moltiplicazione. Siccome 0 soddisfa $0 \cdot (a + bi) = 0$ per ogni $a + bi \in \mathbf{C}$, non può avere un inverso moltiplicativo. Per questa ragione poniamo

$$\mathbf{C}^* = \mathbf{C} - \{0\}.$$

Direttamente dalla definizione si verifica facilmente che la moltiplicazione in \mathbf{C}^* è commutativa. Dimostriamo adesso che \mathbf{C}^* è un gruppo commutativo rispetto alla moltiplicazione con elemento neutro 1.

Verifichiamo l'associatività G_1 : siano $a, b, c, d, e, f \in \mathbf{R}$ e $a + bi, c + di$ e $e + fi$ in \mathbf{C} ; allora

$$\begin{aligned}((a + bi)(c + di))(e + fi) &= ((ac - bd) + (ad + bc)i)(e + fi) \\ &= ((ac - bd)e - (ad + bc)f) + ((ac - bd)f + (ad + bc)e)i \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i \\ (a + bi)((c + di)(e + fi)) &= (a + bi)((ce - df) + (cf + de)i) \\ &= ((a(ce - df) - b(cf + de)) + (a(cf + de) + b(ce - fd))i) \\ &= (ace - adf - bcf - bde) + (acf + ade + bce - bdf)i,\end{aligned}$$

e dunque vale l'associatività della moltiplicazione in \mathbf{C}^* . Osserviamo adesso che per $a + bi \in \mathbf{C}$ si ha

$$(a + bi)(a - bi) = (a^2 + b^2) + (-ab + ba)i = a^2 + b^2.$$

Siccome $a + bi = 0$ se e soltanto se $a^2 + b^2 = 0$, si conclude che per $a + bi \neq 0$

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \right) = 1.$$

Questo implica l'assioma G_3 : ogni $a + bi \in \mathbf{C}^*$ ha un inverso moltiplicativo.

Similmente si verifica che \mathbf{C}^* è chiuso rispetto alla moltiplicazione: siano $a + bi, c + di \in \mathbf{C}^*$. Se $(a + bi)(c + di)$ fosse 0, allora

$$0 = (a - bi)(a + bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2)$$

e dunque $a^2 + b^2 = 0$ oppure $c^2 + d^2 = 0$. Questa è una contraddizione perché $a + bi$ e $c + di$ sono diversi da 0.

Esempio (1.5). *Il gruppo additivo dei vettori.*

Sia n un intero positivo. L'addizione di vettori $\mathbf{v} = (v_1, \dots, v_n)$ e $\mathbf{w} = (w_1, \dots, w_n)$ nello spazio vettoriale \mathbf{R}^n è data da

$$\mathbf{v} + \mathbf{w} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}.$$

Con questa addizione lo spazio vettoriale \mathbf{R}^n diventa un gruppo commutativo. L'elemento neutro è il vettore $\mathbf{0} = (0, \dots, 0)$. L'inverso del vettore $\mathbf{v} = (v_1, \dots, v_n)$ è $-\mathbf{v} = (-v_1, \dots, -v_n)$.

Similmente, si può definire una struttura di gruppo additivo sullo spazio vettoriale complesso \mathbf{C}^n . Per $\mathbf{v} = (v_1, \dots, v_n)$ e $\mathbf{w} = (w_1, \dots, w_n)$ in \mathbf{C}^n si definisce la somma come nel caso di \mathbf{R}^n . Per la teoria degli spazi vettoriali su \mathbf{R} e \mathbf{C} si veda il corso di geometria I.

Esempio (1.6). *Il "Vierergruppe" V_4 di Klein.*

Il gruppo di Klein V_4 contiene 4 elementi: $V_4 = \{e, a, b, c\}$. La moltiplicazione è data dalla seguente tavola:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

L'elemento neutro è e . Si vede che $a^2 = b^2 = c^2 = e$. In altre parole ogni elemento è l'inverso di se stesso. Per verificare l'associatività basta, utilizzando la simmetria del diagramma, distinguere qualche caso. Si lascia la verifica al lettore.

Esempio (1.7). *Il gruppo \mathbf{Z}_n delle classi resto modulo n .*

Sia $n \in \mathbf{Z}$ un intero positivo. Per $k \in \mathbf{Z}$, con $0 \leq k < n$, definiamo

$$R_k = \{a \in \mathbf{Z} : k \text{ è il resto della divisione di } a \text{ per } n\} \quad \text{per } 0 \leq k < n.$$

Per il Teorema 0.1 si ha $\mathbf{Z} = R_0 \cup R_1 \cup \dots \cup R_{n-1}$ e $R_i \cap R_j = \emptyset$ se $i \neq j$. Se $a \in R_k$, si dice che R_k è la classe di congruenza modulo n di a , oppure, brevemente, che R_k è la classe di a . Scriviamo anche \bar{a} per la classe di a e diciamo che a è un rappresentante della classe \bar{a} .

Per $a, b \in \mathbf{Z}$ si ha che $\bar{a} = \bar{b}$ se e soltanto se a e b hanno lo stesso resto della divisione per n e questo è equivalente a dire che n divide $a - b$. In tal caso si dice che a è congruente a b modulo n , oppure che a è uguale a b modulo n e si scrive $a \equiv b \pmod{n}$.

Definiamo

$$\mathbf{Z}_n = \{\bar{a} : a \in \mathbf{Z}\} \quad (\text{indicato anche con } \mathbf{Z}_n)$$

o, equivalentemente,

$$\mathbf{Z}_n = \{R_0, R_1, \dots, R_{n-1}\}.$$

Dunque, gli elementi di \mathbf{Z}_n sono *sottoinsiemi di* \mathbf{Z} . Mettiamo una struttura di gruppo additivo su \mathbf{Z}_n . Definendo

$$\bar{a} + \bar{b} = \overline{a + b}.$$

Questa definizione *non* dipende della scelta di a e b , ma soltanto delle classi \bar{a} e \bar{b} : se prendiamo a' e b' tali che $\bar{a}' = \bar{a}$ e $\bar{b}' = \bar{b}$, allora $a' - a$ e $b' - b$ sono divisibili per n e dunque $(a' + b') - (a + b)$ è divisibile per n , da cui $\overline{a' + b'} = \overline{a + b}$. Si vede dunque che il risultato $\bar{a} + \bar{b}$ non dipende dalla scelta dei rappresentanti delle classi \bar{a} e \bar{b} .

L'operazione è associativa perché l'addizione in \mathbf{Z} è associativa:

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a + b} + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{b + c} = \bar{a} + (\bar{b} + \bar{c}).$$

L'elemento neutro è la classe $\bar{0}$ perché per ogni $\bar{a} \in \mathbf{Z}_n$:

$$\begin{aligned} \bar{0} + \bar{a} &= \overline{0 + a} = \bar{a}, \\ \bar{a} + \bar{0} &= \overline{a + 0} = \bar{a}. \end{aligned}$$

L'inverso della classe \bar{a} è la classe $\overline{-a}$:

$$\begin{aligned} \overline{-a} + \bar{a} &= \overline{(-a) + a} = \bar{0}, \\ \bar{a} + \overline{-a} &= \overline{a + (-a)} = \bar{0}. \end{aligned}$$

Concludiamo che \mathbf{Z}_n è un gruppo con l'addizione. Siccome per $\bar{a}, \bar{b} \in \mathbf{Z}_n$

$$\bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a},$$

il gruppo delle classi resto modulo n è commutativo.

Esempio (1.8). Il gruppo moltiplicativo \mathbf{Z}_n^* delle classi resto modulo n .

Sia n un intero positivo. Definiamo

$$\mathbf{Z}_n^* = \{\bar{a} \in \mathbf{Z}_n : \text{mcd}(a, n) = 1\} \quad (\text{indicato anche con } \mathbf{Z}_n^*).$$

Se $\bar{a}' = \bar{a}$ si ha che n divide $a' - a$; esiste dunque $k \in \mathbf{Z}$ tale che $a' - a = kn$. Per l'Osservazione(0.2)(iii), si ha $\text{mcd}(a', n) = \text{mcd}(a + kn, n) = \text{mcd}(a, n)$. Questo dimostra che l'insieme \mathbf{Z}_n^* è ben definito, cioè il valore di $\text{mcd}(a, n)$ nella definizione non dipende della scelta di a ma soltanto della classe \bar{a} .

Mettiamo una struttura di gruppo moltiplicativo su \mathbf{Z}_n^* . Definiamo

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Verifichiamo che la moltiplicazione è ben definita, ossia non dipende dalle scelte dei rappresentanti a e b : prendiamo a' e b' tali che $\overline{a'} = \overline{a}$ e $\overline{b'} = \overline{b}$, allora $a' - a$ e $b' - b$ sono divisibili per n . Scriviamo $a' = a + kn$ e $b' = b + ln$, per certi $k, l \in \mathbf{Z}$. Quindi

$$a' \cdot b' = (a + kn) \cdot (b + ln) = ab + aln + kbn + kln^2 = ab + (al + kb + kln) \cdot n.$$

Siccome la differenza di $a'b'$ e ab è divisibile per n , le classi \overline{ab} e $\overline{a'b'}$ sono uguali. Concludiamo che la moltiplicazione è ben definita.

L'associatività segue, come nel caso del gruppo additivo \mathbf{Z}_n , dall'associatività in \mathbf{Z} . Si verifica che l'elemento neutro è la classe $\overline{1}$. Dimostriamo che ogni classe $\overline{a} \in \mathbf{Z}_n^*$ ha un inverso: siccome $\text{mcd}(a, n) = 1$, esistono, per il Cor.0.4, interi x, y tali che

$$ax + ny = 1.$$

Questo implica che la differenza di ax e 1 è divisibile per n . In altre parole, le classi $\overline{ax} = \overline{a} \cdot \overline{x}$ e $\overline{1}$ sono uguali e si vede che \overline{x} è l'inverso di \overline{a} . Concludiamo che \mathbf{Z}_n^* è un gruppo moltiplicativo.

Osservazione (1.9). Viceversa, se $\overline{a} \in \mathbf{Z}_n$ ha un inverso moltiplicativo \overline{b} , allora $\overline{a} \overline{b} = \overline{1}$, cioè

$$ab = 1 + kn, \quad \text{per un } k \in \mathbf{Z}.$$

In altre parole, \mathbf{Z}_n^* è formato da tutte e sole le classi $\overline{x} \in \mathbf{Z}_n$ che ammettono inverso moltiplicativo.

La *funzione di Eulero* è la funzione che ad un intero positivo associa la cardinalità del gruppo moltiplicativo \mathbf{Z}_n^* :

$$\varphi(n) = \#\mathbf{Z}_n^*,$$

ossia $\varphi(n) = \#\{a \in \{1, 2, \dots, n\} : \text{mcd}(a, n) = 1\}$. Ad esempio, per $n = 12$ si trova $\varphi(12) = 4$ e la tavola moltiplicativa di \mathbf{Z}_{12}^* è data da

	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Si vede che è la "stessa" tavola del gruppo di Klein (Esempio(1.6)). Siccome la moltiplicazione di \mathbf{Z}_{12}^* è associativa, abbiamo gratis una dimostrazione dal fatto che l'operazione del gruppo V_4 di Klein è associativa.

Esercizio. Stabilire se esiste l'inverso di a modulo n e, in caso affermativo, determinarlo, dove a ed n sono dati da:

- (a) $a = 11$ e $n = 13$; (c) $a = 21$ e $n = 6$; (e) $a = -8$ e $n = 15$;
 (b) $a = 6$ e $n = 21$; (d) $a = 27$ e $n = 36$; (f) $a = 144$ e $n = 233$.

Gruppi abeliani finiti.

Teorema(1.10). (Teorema di Lagrange). Sia G un gruppo abeliano finito con n elementi. Allora

$$g^n = g \circ \dots \circ g = e, \quad \forall g \in G.$$

Dimostrazione. Consideriamo il prodotto di tutti gli elementi di G

$$\prod_{g \in G} g.$$

Se h è un qualunque elemento di G fissato, valgono le seguenti identità

$$\prod_{g \in G} g = \prod_{g \in G} hg = h^n \prod_{g \in G} g. \quad (1.1)$$

La prima identità vale perché l'applicazione $L_h: G \rightarrow G$, $g \mapsto hg$ è una bigezione da G in G e dunque induce semplicemente una permutazione di G . La seconda vale perché G è abeliano e quindi possiamo raccogliere tutti i fattori h a sinistra. Se moltiplichiamo i termini dell'identità (1.1) a destra per $(\prod_{g \in G} g)^{-1}$, troviamo il risultato cercato: $h^n = e$, per ogni $h \in G$.

Sia G un gruppo abeliano finito di n elementi e sia $g \in G$. Diciamo che g ha ordine m , e lo indichiamo con $\text{ord}(g) = m$, se m è il più piccolo intero positivo per cui vale $g^m = e$. Per il Teorema di Lagrange, si ha che $m \leq n$.

Corollario (1.11). Sia G un gruppo abeliano finito con n elementi. Allora l'ordine di un qualunque elemento $g \in G$ divide n .

Dimostrazione. Sia $g \in G$ e sia $m = \text{ord}(g)$. Supponiamo per assurdo che m non divida n , ossia che risulti $n = mq + r$, con $0 < r < m$. Per definizione $g^m = e$ e per il teorema di Lagrange $g^n = e$. Ne segue che

$$e = g^n = g^{mq+r} = (g^m)^q g^r = g^r,$$

contro l'ipotesi di minimalità di m . Dunque r è necessariamente uguale a zero ed m divide n .

Nel caso dei gruppi finiti \mathbf{Z}_n^* , la cui cardinalità è data dalla funzione di Eulero $\varphi(n)$, il teorema di Lagrange dice

$$\bar{x}^{\varphi(n)} \equiv \bar{1} \text{ in } \mathbf{Z}_n^*, \quad \text{per ogni } \bar{x} \in \mathbf{Z}_n^*. \quad (1.2)$$

In particolare, se p è un numero primo, vale $\varphi(p) = p - 1$ e la (1.2) è conosciuta anche come il Piccolo Teorema di Fermat.

Teorema(1.12). (Piccolo Teorema di Fermat). Sia p un numero primo. Sia x un intero con $\text{mcd}(x, p) = 1$. Allora

$$x^{p-1} \equiv 1 \pmod{p}.$$

Esercizio(1.13). Sia $n = pq$, con p, q numeri primi. Allora vale

$$x^{(p-1)(q-1)} \equiv 1 \pmod{n}, \quad \text{per ogni intero } x \text{ con } \text{mcd}(x, n) = 1.$$

Soluzione. Osserviamo innanzitutto che se $n = pq$, con p, q primi, la condizione $\text{mcd}(x, n) = 1$ implica $\text{mcd}(x, p) = \text{mcd}(x, q) = 1$. Di conseguenza $\bar{x} \in \mathbf{Z}_p^*$ e $\bar{x} \in \mathbf{Z}_q^*$. Applicando nei due casi il Piccolo Teorema di Fermat, otteniamo

$$x^{(p-1)} \equiv 1 \pmod{p}, \quad x^{(q-1)} \equiv 1 \pmod{q}.$$

In particolare, x soddisfa il sistema di congruenze

$$\begin{cases} x^{(p-1)(q-1)} \equiv 1 \pmod{p} \\ x^{(p-1)(q-1)} \equiv 1 \pmod{q} \end{cases}$$

equivalente alla singola congruenza

$$x^{(p-1)(q-1)} \equiv 1 \pmod{n}, \quad n = pq.$$

Esercizio(1.14). Dimostrare: ogni numero n tale che $\text{mcd}(n, 10) = 1$ divide un intero non nullo che ha tutte le cifre uguali. Per esempio: 219 divide 33333333.

Soluzione. Se $\text{mcd}(n, 10) = 1$, allora $\bar{10} \in \mathbf{Z}_n^*$ e, per il teorema di Lagrange, esiste $k \in \mathbf{Z}$ tale che $10^k \equiv 1 \pmod{n}$. Ne segue che $10^k - 1 \equiv 0 \pmod{n}$, ossia che n divide $10^k - 1$. Poiché $10^k - 1$ è un numero con tutte le cifre uguali a 9, la tesi è dimostrata.

Sia ora $n = 219$. Si verifica facilmente che $219 = 3 \cdot 73$ e che $\text{mcd}(10, 219) = 1$. Dunque $\bar{10} \in \mathbf{Z}_{219}^*$. Per determinare l'ordine di $\bar{10}$ in \mathbf{Z}_{219}^* , osserviamo che per il Teorema Cinese del Resto

$$10^k \equiv 1 \pmod{219} \Leftrightarrow \begin{cases} 10^k \equiv 1 \pmod{3} \\ 10^k \equiv 1 \pmod{73} \end{cases}.$$

Inoltre, poiché $10 \equiv 1 \pmod{3}$, basta calcolare potenze di 10 modulo 73:

$$\bar{10}, \quad \bar{10}^2 = \bar{27}, \quad \bar{10}^3 = \bar{51}, \quad \bar{10}^4 = \bar{72} = \bar{-1}, \quad \bar{10}^8 = \bar{1}.$$

Dunque l'ordine di $\bar{10}$ in \mathbf{Z}_{73} e in \mathbf{Z}_{219} è uguale a 8 e 219 divide $10^8 - 1 = 99999999$. Infine, poiché 219 ha il fattore 3 con molteplicità uno, mentre 99999999 ha il fattore 3 con molteplicità due, si ha che 219 divide anche 33333333, come richiesto.

Esercizio(1.15). Sia p un primo e sia $a \in \mathbf{Z}$.

(a) Dimostrare che

$$a^{k(p-1)+1} \equiv a \pmod{p},$$

per ogni intero $k \geq 0$.

(b) Provare che $a^{13} - a$ è divisibile per 2730, per ogni $a \in \mathbf{Z}$.

Soluzione.

(a) Osserviamo innanzitutto che la congruenza richiesta è soddisfatta per ogni $a \equiv 0 \pmod{p}$. Se invece $a \not\equiv 0 \pmod{p}$, allora $\bar{a} \in \mathbf{Z}_p^*$ e per il Piccolo Teorema di Fermat vale

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

In particolare, per ogni $k \in \mathbf{Z}$, vale $a^{k(p-1)} \equiv 1 \pmod{p}$ e, moltiplicando ambo i termini della congruenza per a , vale

$$a^{k(p-1)+1} \equiv a \pmod{p},$$

come richiesto.

(b) Provare che $a^{13} - a$ è divisibile per 2730, per ogni $a \in \mathbf{Z}$, equivale a provare che

$$a^{13} - a \equiv 0 \pmod{2730}$$

ossia che

$$a^{13} \equiv a \pmod{2730}. \quad (*)$$

Poiché $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, per il Teorema Cinese del Resto, la congruenza (*) è equivalente al sistema di congruenze

$$\begin{cases} a^{13} \equiv a \pmod{2} \\ a^{13} \equiv a \pmod{3} \\ a^{13} \equiv a \pmod{5} \\ a^{13} \equiv a \pmod{7} \\ a^{13} \equiv a \pmod{13}. \end{cases}$$

Applicando il risultato del punto (a) alle singole congruenze del sistema, troviamo che ogni $a \in \mathbf{Z}$ soddisfa il sistema e la congruenza (*), come richiesto.

Calcolo di potenze di interi modulo n .

I risultati precedenti possono essere usati ad esempio per calcolare grosse potenze di interi modulo n , quando n è un numero primo o il prodotto di primi distinti non troppo grandi.

Esercizio(1.16). Calcolare il resto della divisione per 5 del numero $33213457^{27221447139^{122222281}}$.

Soluzione. Il problema chiede la classe resto in \mathbf{Z}_5 del numero a^b , dove $a = 33213457$ e $b = 27221447139^{122222281}$. Innanzitutto osserviamo che $a^b \equiv \bar{a}^b$ in \mathbf{Z}_5 e che nel nostro caso $\bar{a} \equiv \bar{2}$ in \mathbf{Z}_5 . Inoltre, poiché 5 è un numero primo, il gruppo moltiplicativo \mathbf{Z}_5^* ha cardinalità $\varphi(5) = 4$. Dal teorema di Lagrange segue che

$$\bar{a}^4 \equiv \bar{2}^4 \equiv \bar{1}, \quad \text{in } \mathbf{Z}_5.$$

In particolare, se $b = 4q + r$, segue che

$$\bar{a}^{4q+r} \equiv (\bar{a}^4)^q \bar{a}^r \equiv \bar{a}^r, \quad \text{in } \mathbf{Z}_5.$$

Dunque, ai fini del nostro calcolo, quella che conta è solo la classe resto r di b modulo 4. Con un ragionamento analogo a quello sopra e tenendo conto che $\varphi(4) = 2$, troviamo che

$$\bar{b} \equiv \overline{27221447139^{122222281}} \equiv \bar{3}^{122222281} \equiv \bar{3}^{2q+1} \equiv \bar{3}, \quad \text{in } \mathbf{Z}_4.$$

In conclusione, $r = 3$ e

$$\bar{a}^b \equiv \bar{2}^3 \equiv \bar{8} \equiv \bar{3}, \quad \text{in } \mathbf{Z}_5.$$

Esercizio(1.17). Calcolare il resto della divisione per 15 del numero 33^{27} .

Soluzione. Sia x il resto della divisione per 15 del numero 33^{27} . Per definizione, x è l'intero fra 0 e 14 che soddisfa $x \equiv 33^{27} \pmod{15}$. Poiché $15 = 3 \cdot 5$, con $\text{mcd}(3, 5) = 1$, vale l'equivalenza

$$x \equiv 33^{27} \pmod{15} \quad \Leftrightarrow \quad \begin{cases} x \equiv 33^{27} \pmod{3} \\ x \equiv 33^{27} \pmod{5}. \end{cases}$$

Il vantaggio di questa riduzione sta nel fatto che, conoscendo $\varphi(3) = 2$ e $\varphi(5) = 4$, possiamo calcolare $33^{27} \pmod{3}$ e $33^{27} \pmod{5}$ ottenendo

$$\begin{cases} x \equiv 33^{27} \pmod{3} \\ x \equiv 33^{27} \pmod{5} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 2 \pmod{5}. \end{cases}$$

Per il Teorema Cineste del Resto, il sistema ha soluzioni in \mathbf{Z} che sono della forma $x = x_0 + k15$, $k \in \mathbf{Z}$. Il resto cercato è l'unica soluzione x del sistema fra 0 e 14.

In generale, dal punto di vista computazionale, il metodo più efficiente per calcolare grosse potenze di interi modulo n (con n arbitrario) è quello di convertire l'esponente in forma binaria. Il risultato si ottiene poi mediante successive elevazioni al quadrato modulo n e moltiplicazioni (vedi R. Schoof, Fattorizzazione e crittosistemi a chiave pubblica, Didattica delle Scienze, 1988).

Test di primalità.

Il Piccolo Teorema di Fermat può essere usato per escludere che un numero intero sia primo: se n è un intero positivo e risulta

$$a^{n-1} \not\equiv 1 \pmod{n},$$

per qualche intero a con $\text{mcd}(n, a) = 1$, certamente n non è un numero primo.

Esistono comunque dei numeri n non primi con la proprietà che

$$a^{n-1} \equiv 1 \pmod{n},$$

per ogni intero a con $\text{mcd}(a, n) = 1$. Chiaramente è sufficiente considerare $0 \leq a \leq n - 1$.

Questi numeri si chiamano *numeri di Carmichael*. Eccone alcuni: 561, 1729, 2465, 2821, 6601, 8911.....

I numeri di Carmichael sono infiniti e sono caratterizzati dalle seguenti proprietà:

Criterio di Korselt: *Un intero positivo n è un numero di Carmichael se e solo se*

- (i) n è privo di fattori quadratici;
- (ii) se un numero p divide n , allora $p - 1$ divide $n - 1$.

In pratica, nei test di primalità viene usata una versione raffinata del Piccolo Teorema di Fermat:

Teorema 1.18. (Miller-Rabin) *Sia n un numero primo dispari. Siano m un numero dispari e k un intero tali che $n - 1 = m2^k$. Sia a un intero con $\text{mcd}(a, n) = 1$ e sia $b = a^m$. Allora $b^{2^k} \equiv 1 \pmod{n}$ e si hanno due possibilità:*

- (i) $b \equiv 1 \pmod{n}$;
- (ii) $b \not\equiv 1 \pmod{n}$; se i è il più piccolo intero tale che $b^{2^i} \equiv 1 \pmod{n}$, allora $b^{2^{i-1}} \equiv -1 \pmod{n}$.

Un numero n che per un numero a , con $\text{mcd}(a, n) = 1$, soddisfa una delle condizioni (i) (ii), si dice *a-pseudoprimo* e si dice *pseudoprimo* se soddisfa una delle condizioni (i) (ii), per ogni numero a . con $\text{mcd}(a, n) = 1$ e $0 \leq a \leq n - 1$. Un numero non primo n ha al più il 25% delle probabilità di passare il test di Miller-Rabin. Di fatto, molte di meno; così che un numero *a-pseudoprimo* anche per pochi a è quasi-certamente un numero primo. Questo è sufficiente per gran parte delle applicazioni commerciali.

Perché il Teorema di Miller-Rabin funziona meglio del Piccolo Teorema di Fermat come test di primalità? La differenza sta nella condizione (ii). Il Teorema di Miller-Rabin sfrutta oltre alla cardinalità del gruppo moltiplicativo \mathbf{Z}_n^* , il fatto seguente (vedi Esercizio (2.9)):

Se n è primo, allora la congruenza $x^2 \equiv 1 \pmod{n}$ ha esattamente due soluzioni modulo n :

$$x \equiv 1 \pmod{n}, \quad x \equiv -1 \pmod{n}.$$

Esempio 1.19. Illustriamo il test di primalità basato sul Teorema di Miller-Rabin sul numero di Carmichael $n = 561 = 3 \cdot 11 \cdot 17$.

Scriviamo $n - 1 = 560 = 352^4$. Dunque $m = 35$ e $k = 16$.

Scegliamo ad esempio $a = 2$ (per semplicità di calcolo).

Calcoliamo innanzitutto

$$b = a^m = 2^{35} \equiv 263 \pmod{561}.$$

Poiché $b \not\equiv 1 \pmod{561}$, proseguiamo il test calcolando le potenze del tipo $b^{2^i} \pmod{561}$:

$$b^2 \equiv 166 \pmod{561}, \quad b^{2^2} = b^2 \cdot b^2 \equiv 67 \pmod{561}, \quad b^{2^3} = b^{2^2} \cdot b^2 \equiv 1 \pmod{561}.$$

Troviamo $b^{2^3} \equiv 1 \pmod{561}$, ma $b^{2^2} \not\equiv -1 \pmod{561}$. Dunque n non è primo.

Osservazione 1.20. Per $n = 561 = 3 \cdot 11 \cdot 17$, si ha

$$x^2 \equiv 1 \pmod{561} \Leftrightarrow \begin{cases} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv 1 \pmod{11} \\ x^2 \equiv 1 \pmod{17}; \end{cases}$$

Ognuna delle congruenze del sistema (con modulo primo) ha due soluzioni $x \equiv \pm 1$, per cui le soluzioni del sistema sono date dall'unione delle soluzioni degli *otto* sistemi

$$\begin{cases} x \equiv \pm 1 \pmod{3} \\ x \equiv \pm 1 \pmod{11} \\ x \equiv \pm 1 \pmod{17}. \end{cases}$$

Per il Teorema Cinese del Resto ognuno di essi ha un'unica soluzione modulo $n = 561$, e dunque la congruenza $x^2 \equiv 1 \pmod{561}$ ha otto soluzioni distinte modulo $n = 561$. Fra esse ci sono sempre $x \equiv 1, -1 \pmod{561}$. Ad esempio, la soluzione $x \equiv 67 \pmod{561}$ che abbiamo trovato durante il test di Miller-Rabin corrisponde al sistema

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{11} \\ x \equiv -1 \pmod{17}, \end{cases}$$

un'altra è $x \equiv 188 \pmod{561}$ e corrisponde al sistema

$$\begin{cases} x \equiv -1 \pmod{3} \\ x \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{17}. \end{cases}$$

Esempio 1.21. Sia $n = 7933$. Scriviamo $n - 1 = 7932 = 19832^2$. Dunque $m = 1983$ e $k = 2$.

Scegliamo $a = 2$. Troviamo

$$b = a^m = 2^{1983} \equiv 4933 \pmod{7933}.$$

Poiché $b \not\equiv 1 \pmod{7933}$, proseguiamo il test calcolando le potenze del tipo $b^{2^i} \pmod{7933}$:

$$b^2 \equiv 7932 \equiv -1 \pmod{7933}, \quad b^{2^2} = b^2 \cdot b^2 \equiv 1 \pmod{7933}.$$

Conclusione: 7933 è 2-pseudoprimo.

Scegliamo $a = 3$. Troviamo

$$b = a^m = 3^{1983} \equiv 7932 \pmod{7933}.$$

Poiché $b \equiv -1 \pmod{7933}$, calcolando le potenze del tipo $b^{2^i} \pmod{7933}$ troviamo

$$b^2 \equiv 1 \pmod{7933}.$$

Conclusione: 7933 è 3-pseudoprimo.

Possiamo proseguire il test, scegliendo altri numeri primi a . Ogni volta che il numero passa il test per un nuovo a , aumenta la sua probabilità di essere primo. In questo caso, $n = 7933$ è primo ed è precisamente il 1002-simo numero primo.

2. Anelli e campi.

In questo paragrafo introduciamo gli *anelli* e i *campi* e ne diamo diversi esempi importanti.

Definizione. Un anello R è un insieme fornito di due operazioni, *addizione* “+” e *moltiplicazione* “·”, che soddisfano i seguenti assiomi:

(R_1) (*Gruppo additivo*) L'insieme $(R, +)$ è un gruppo *abeliano*.

(R_2) (*Associatività*) Per ogni $x, y, z \in R$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

(R_3) (*L'identità*) Esiste un elemento $1 \in R$, con la proprietà che per ogni $x \in R$

$$1 \cdot x = x \cdot 1 = x.$$

(R_4) (*Distributività*) Per ogni $x, y, z \in R$

$$\begin{aligned}x \cdot (y + z) &= x \cdot y + x \cdot z, \\(y + z) \cdot x &= y \cdot x + z \cdot x.\end{aligned}$$

Se *in aggiunta* vale l'assioma

(R_5) (*Commutatività*) Per ogni $x, y \in R$

$$x \cdot y = y \cdot x,$$

l'anello R si dice *commutativo*.

Se *in aggiunta* valgono l'assioma (R_5) e l'assioma

(R_6) (*Inverso moltiplicativo*) Per ogni $x \in R$, $x \neq 0$ esiste $x^* \in R$ tale che

$$x \cdot x^* = x^* \cdot x = 1.$$

l'anello R si dice un *campo*.

Osservazione. Esistono anelli non commutativi, ed esistono anelli in cui non tutti gli elementi $x \neq 0$ sono invertibili.

Esempio (2.1). Con l'addizione e la moltiplicazione introdotte nella sezione 1, gli insiemi \mathbf{Z} , \mathbf{Q} , \mathbf{R} e \mathbf{C} sono anelli. Lasciamo al lettore la facile verifica. Gli anelli \mathbf{Z} , \mathbf{Q} , \mathbf{R} e \mathbf{C} sono commutativi. Solo gli anelli \mathbf{Q} , \mathbf{R} e \mathbf{C} sono campi.

Esempio (2.2). (*L'anello banale*) Di solito, in un anello R gli elementi 0 e 1 sono distinti. Se invece $0 = 1$, ogni elemento di R è uguale a 0, perché per $x \in R$ vale

$$x = 1 \cdot x = 0 \cdot x = 0.$$

Dunque, se $0 = 1$, l'anello R è uguale a $\{0\}$ e si chiama *l'anello banale*.

Esempio (2.3). (*L'anello \mathbf{Z}_n delle classi resto modulo n*) Con l'addizione definita nell'Esempio 1.7 e la moltiplicazione data da

$$\bar{a} \cdot \bar{b} = \overline{ab},$$

l'insieme \mathbf{Z}_n è un anello commutativo. Lasciamo le verifiche al lettore.

Esempio (2.4). (*L'anello degli interi di Gauss*) Sia $\mathbf{Z}[i]$ il sottoinsieme di \mathbf{C} dato da

$$\mathbf{Z}[i] = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Z}\}.$$

È facile verificare che $\mathbf{Z}[i]$ con l'addizione e la moltiplicazione di \mathbf{C} è un anello commutativo.

Definizione. Sia R un anello. Un'*unità* di R è un elemento che ammette inverso moltiplicativo, ossia un elemento $x \in R$ per cui esiste $x^* \in R$ con

$$x \cdot x^* = x^* \cdot x = 1.$$

L'inverso x^* di un elemento $x \in R$ è unico. A volte si indica con x^{-1} . L'insieme delle unità di R si indica con R^* .

Proposizione (2.5). *Sia R un anello. Le unità di R formano un gruppo moltiplicativo.*

Dimostrazione. Ovviamente vale l'assioma dell'associatività. L'identità 1 è l'elemento neutro di R^* . Direttamente dalla definizione di inverso si ha che se $a \in R^*$, allora $a^{-1} \in R^*$. Infine, se $a, b \in R^*$, allora il prodotto $ab \in R^*$, in quanto

$$(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1.$$

Dunque R^* è un gruppo moltiplicativo.

Definizione. Sia R un anello commutativo. Un elemento $a \in R$ si dice un *divisore di zero* se esiste $b \in R$ con $b \neq 0$ tale che $ab = 0$.

Proposizione (2.7). *Un divisore di zero in un anello R non può essere un'unità.*

Dimostrazione. Supponiamo che a sia un divisore di zero ed anche un'unità. Dunque esistono elementi $b, c \in R$ con

$$ab = 0, \quad (b \neq 0) \quad \text{e} \quad ca = 1.$$

Abbiamo

$$0 = c \cdot 0 = c \cdot (ab) = (ca) \cdot b = 1 \cdot b = b,$$

contro l'ipotesi che $b \neq 0$.

Osservazione. A causa dell'esistenza di divisori di zero, in generale in un anello *non vale la legge di cancellazione*:

$$xy = xz, \quad x \in R \setminus \{0\} \quad \not\Rightarrow \quad y = z.$$

Esempio. Le unità negli anelli \mathbf{Q} , \mathbf{R} e \mathbf{C} coincidono rispettivamente con \mathbf{Q}^* , \mathbf{R}^* e \mathbf{C}^* , introdotti nel paragrafo 1. Il gruppo \mathbf{Z}^* è uguale a $\{+1, -1\}$, mentre $\mathbf{Z}[i]^* = \{\pm 1, \pm i\}$. Negli anelli \mathbf{Z} , \mathbf{Q} , \mathbf{R} non ci sono divisori di zero.

Esempio. Le unità nell'anello \mathbf{Z}_n coincidono con \mathbf{Z}_n^* (vedi Esempio (1.8) e Osservazione (1.9)). Nell'anello \mathbf{Z}_n , ci sono sempre divisori di zero quando n non è primo. Per esempio, in \mathbf{Z}_6 si ha $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$.

Proposizione (2.6). Sia n un intero positivo. L'anello \mathbf{Z}_n è un campo se e soltanto se n è un numero primo.

Dimostrazione. L'anello \mathbf{Z}_n è un campo se e soltanto se ogni classe $\bar{x} \neq \bar{0}$ ha un inverso moltiplicativo, ossia se e soltanto se

$$\mathbf{Z}_n^* = \mathbf{Z}_n - \{0\}.$$

Ciò equivale a richiedere che per ogni $a \in \mathbf{Z}$, con $0 < a < n$, sia $\text{mcd}(a, n) = 1$. Questo vale se e soltanto se n è un numero primo, come richiesto.

Osservazione 2.7. Una congruenza modulo n può essere interpretata come un'equazione in \mathbf{Z}_n ; viceversa, ad un'equazione in \mathbf{Z}_n corrisponde una congruenza modulo n . Consideriamo ad esempio un'equazione di primo grado

$$\bar{a}\bar{x} \equiv \bar{b}, \quad \text{in } \mathbf{Z}_n. \quad (2.1)$$

Allora valgono i seguenti risultati:

- (a) L'equazione ammette soluzione se e solo se $\text{mcd}(a, n)$ divide b ;
- (b) Sia $d = \text{mcd}(a, n)$ e supponiamo che d divida b . Allora l'equazione ha esattamente d soluzioni distinte in \mathbf{Z}_n .

Dimostrazione. (a) segue direttamente dalla Proposizione (0.16).

(b) Se $d = \text{mcd}(a, n)$ divide b , allora la congruenza che corrisponde all'equazione (2.1) è equivalente a

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}, \quad \text{mcd}\left(\frac{a}{d}, \frac{n}{d}\right) = 1.$$

La soluzione generale di questa congruenza è della forma $x = x_0 + M\frac{n}{d}$, dove $0 \leq x_0 \leq (\frac{n}{d} - 1)$ ed $M \in \mathbf{Z}$. Concludiamo osservando che al variare di $M = 0, 1, \dots, d - 1$ gli interi

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{n}{d}2, \quad \dots, \quad x_0 + \frac{n}{d}(d - 1)$$

sono tutti distinti modulo n , e per ogni altro valore di M non ne otteniamo altri di nuovi.

Osservazione 2.7. Se $d = 1$, l'equazione ha un'unica soluzione: la condizione $d = 1$ equivale all'invertibilità di \bar{a} in \mathbf{Z}_n e l'unica soluzione è data da $x = \bar{a}^{-1}\bar{b}$.

Se d divide b e $d > 1$, l'elemento \bar{a} non è invertibile in \mathbf{Z}_n . A riprova del fatto che per \bar{a} non vale la legge di cancellazione, l'equazione ha diverse soluzioni distinte in \mathbf{Z}_n .

Esercizio 2.8. Determinare tutte le soluzioni dell'equazione $\bar{4} \cdot \bar{x} \equiv \bar{8}$ in \mathbf{Z}_{24} .

Soluzione. La congruenza corrispondente è data da

$$4x \equiv 8 \pmod{24},$$

che ha soluzione, in quanto $4 = \text{mcd}(4, 24)$ divide 8, ed è equivalente alla congruenza

$$x \equiv 2 \pmod{6}.$$

Le soluzioni di quest'ultima congruenza sono $x = 2 + 6M$, al variare di $M \in \mathbf{Z}$. Per $M = 0, 1, 2, 3$ troviamo $x = 2, 8, 14, 20$ che corrispondono alle quattro soluzioni distinte dell'equazione originaria

$$\bar{2}, \bar{8}, \bar{14}, \bar{20} \in \mathbf{Z}_{24}.$$

Esercizio 2.9. Sia n un numero primo. Allora

$$x^2 \equiv 1 \pmod{n} \quad \Leftrightarrow \quad x \equiv 1 \pmod{n} \quad \text{oppure} \quad x \equiv -1 \pmod{n}.$$

In altre parole, l'equazione $\bar{x}^2 \equiv \bar{1}$ ha esattamente le due soluzioni $\bar{x} = \bar{1}, \overline{-1}$ in \mathbf{Z}_n .

Soluzione. La congruenza $x^2 \equiv 1 \pmod{n}$ è equivalente a $(x+1)(x-1) \equiv 0 \pmod{n}$. Poiché n divide $(x+1)(x-1)$ se e solo se divide almeno uno dei fattori, le soluzioni della congruenza sono

$$x = 1 + hn \quad \text{e} \quad x = -1 + hn, \quad h, k \in \mathbf{Z}.$$

Quindi $\bar{1}$ e $\overline{-1}$ sono le due soluzioni dell'equazione $\bar{x}^2 \equiv \bar{1}$ in \mathbf{Z}_n .