3.3 Congruenze e aritmetica modulare

Basandoci sui fatti mostrati nei paragrafi precedenti di questo capitolo, introdurremo e studieremo ora un'importante relazione di equivalenza sull'insieme dei numeri interi, la cosiddetta *congruenza modulo n*.

Definizione 3.20. Sia n un intero positivo fissato. Dati $a, b \in \mathbb{Z}$, diremo che a è *congruo a b modulo n* se a e b divisi per n danno lo stesso resto; equivalentemente, a è congruo a b modulo n se la differenza $a - b$ è un multiplo di n.

Che le due formulazioni della definizione appena data siano equivalenti si vede facilmente: infatti, da una parte, se a e b divisi per n danno lo stesso resto, ovvero $a = nq_1 + r$ e $b = nq_2 + r$, allora

$$a - b = (nq_1 + r) - (nq_2 + r) = nq_1 + r - nq_2 - r = nq_1 - nq_2 = n(q_1 - q_2)$$

ovvero la differenza $a - b$ è un multiplo di n.
Viceversa, supponiamo che $a - b = kn$ per qualche k, ovvero $a = b + kn$. Se il resto della divisione di b per n è r, ovvero $b = nq + r$, allora sostituendo in $a = b + kn$ si trova

$$a = b + kn = nq + r + kn = n(q + k) + r$$

Da cui si vede che anche a, divisa per n, ha resto r (con quoziente $q + k$).

Per indicare che a è congruo a b modulo n, scriveremo

$$a \equiv b (mod\ n)$$

o anche

$$a \equiv_n b$$

Mostriamo ora che la congruenza è una relazione di equivalenza, ovvero che gode delle proprietà riflessiva, simmetrica e transitiva (Definizione 2.6): intanto, si ha

$$a - a = 0 = 0 \cdot n$$

ovvero la differenza tra a e se stesso è un multiplo di n: per la definizione data, questo significa che $a \equiv_n a$, ovvero la congruenza è riflessiva.
Inoltre, se $a \equiv_n b$, ovvero $a - b = kn$ per qualche $k \in \mathbb{Z}$, si ha, semplicemente cambiando di segno,

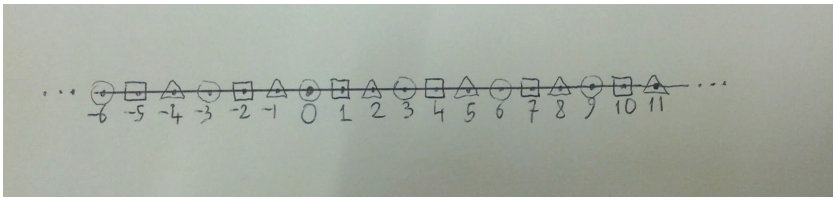
$$b - a = -kn = (-k)n$$

ovvero anche $b - a$ è un multiplo di n, cioè $b \equiv_n a$: la relazione è anche simmetrica.
Infine, se $a \equiv_n b$ (ovvero $a - b = kn$ per qualche $k \in \mathbb{Z}$) e $b \equiv_n c$ (ovvero $b - c = ln$ per qualche $l \in \mathbb{Z}$) allora si ha

$$a - c = a - b + b - c = kn + ln = (k + l)n$$

ovvero anche $a - c$ è un multiplo di n, cioè $a \equiv_n c$: la relazione è anche transitiva.

In base alla teoria vista nel capitolo precedente, tale relazione ripartisce allora $\mathbb{Z}$ in classi di equivalenza non vuote e disgiunte: in ogni classe vi sono tutti i numeri interi che hanno lo stesso resto quando li si divide per n.
Dal momento che il resto r della divisione per n deve soddisfare $0 \leq r < n$, i possibili resti sono $0, 1, 2, \ldots, n - 1$, quindi avremo esattamente n classi di equivalenza: $[0], [1], \ldots, [n - 1]$. L'insieme $\{[0], [1], \ldots, [n - 1]\}$ delle classi di equivalenza su $\mathbb{Z}$ della congruenza modulo n si denota anche $\mathbb{Z}_n$.
Ad esempio, sia $n = 3$: i possibili resti della divisione per 3 sono $0, 1, 2$. La classe $[0]$ di equivalenza di 0 contiene tutti i numeri a tali che $a = a - 0 = 3k$, ovvero i multipli di 3; la classe $[1]$ di equivalenza di 1 contiene tutti gli interi a tali che $a - 1 = 3k$, ovvero $a = 3k + 1$ (ad esempio 4, 7, 10, -2, -5 etc.); la classe $[2]$ di equivalenza di 2 contiene tutti gli interi a tali che $a - 2 = 3k$, ovvero $a = 3k + 2$ (ad esempio 5, 8, 11, -1, -4 etc.)



(stiamo etichettando con lo stesso simbolo interi che stanno nella stessa classe).

Se $n = 2$, abbiamo solo due resti possibili, 0 e 1 e quindi due classi, $[0]$ e $[1]$: la prima contiene tutti gli interi a del tipo $2k$ e la seconda tutti gli interi del tipo $2k + 1$, ovvero la partizione indotta su $\mathbb{Z}$ è quella in numeri pari e numeri dispari.

Come tutte le relazioni di equivalenza, la relazione di congruenza è una sorta di "uguaglianza in senso largo": consideriamo due numeri "uguali" se lo sono "a meno di mutipli di n".

Ora, la relazione di equivalenza per eccellenza, l'uguaglianza, verifica l'ovvia proprietà che se $a = b$ e $a' = b'$ allora $a + a' = b + b'$ e $aa' = bb'$: vediamo ora che anche la congruenza modulo n si comporta esattamente nello stesso modo:

Teorema 3.21. La congruenza modulo n verifica le due seguenti proprietà:

(1) se $a \equiv_n b$ e $a' \equiv_n b'$, allora $a + a' \equiv_n b + b'$

(2) se $a \equiv_n b$ e $a' \equiv_n b'$, allora $aa' \equiv_n bb'$

Proof. Dimostriamo la (1): se $a \equiv_n b$ e $a' \equiv_n b'$ allora vuol dire che $a - b = kn$ e $a' - b' = ln$ per qualche $k, l \in \mathbb{Z}$; dobbiamo dimostrare che anche la differenza tra $a + a'$ e $b + b'$ è un multiplo di n. Ma infatti

$$a + a' - (b + b') = a - b + a' - b' = kn + ln = (k + l)n$$

come volevamo. Ora, per dimostrare la (2), sotto la stessa ipotesi dobbiamo dimostrare che la differenza tra aa' e bb' è un multiplo di n, ovvero equivalentemente che $aa' = bb' + qn$ per qualche $q \in \mathbb{Z}$. Usando $a - b = kn$ e $a' - b' = ln$ (riscrivibili come $a = b + kn$ e $a' = b' + ln$) abbiamo

$$aa' = (b + kn)(b' + ln) = bb' + bln + knb' + kln^2 = bb' + n(bl + kb' + kln)$$

il che dimostra l'asserto (con $q = bl + kb' + kln$). □

Le due proprietà appena dimostrate, come vedremo, hanno molte applicazioni.
La prima che citiamo è la dimostrazione di alcuni criteri di divisibilità: ad esempio, è noto che un numero n è divisibile per 3 se e solo se la somma delle sue cifre è divisibile per 3 (stesso enunciato vale per 9).
Ad esempio, il numero $n = 1917$ è divisibile per 3 in quanto lo è la somma $1+9+1+7 = 18$ delle sue cifre; il numero 313 non lo è perché $3+1+3 = 10$ non lo è.
La spiegazione di tale criterio si basa proprio sul Teorema 3.21: infatti, dire che le cifre di n (nella notazione decimale) sono $a_k, a_{k-1}, \ldots, a_1, a_0$ significa dire che

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \tag{3.36}$$

Ora, poiché $10 = 3 \cdot 3 + 1$, si ha $10 \equiv_3 1$; applicando la (2) del Teorema 3.21 al particolare caso $a = a' = 10$, $b = b' = 1$, si ha che $10 \cdot 10 \equiv_3 1 \cdot 1$, ovvero $10^2 \equiv_3 1$; sempre applicando la stessa proprietà, si ha $10^2 \cdot 10 \equiv_3 1 \cdot 1$, ovvero

$10^3 \equiv_3 1$ e così via si vede che tutte le potenze positive 10^i di 10 sono congrue a 1 modulo 3.
Ora, questo implica che per ogni addendo della rappresentazione (3.36), che è del tipo $a_i 10^i$, sia $a_i 10^i \equiv_3 a_i$: infatti, applicando di nuovo la (2) del Teorema 3.21, si ha che $a_i \equiv_3 a_i$ (la congruenza gode della proprietà riflessiva) e $10^i \equiv_3 1$ implicano proprio $a_i \cdot 10^i \equiv_3 a_i \cdot 1$.
A questo punto, poichè $a_k 10^k \equiv_3 a_k$, $a_{k-1} 10^{k-1} \equiv_3 a_{k-1}$ e così via fino a $a_1 10 \equiv_3 a_1$ (l'ultima, $a_0 \equiv_3 a_0$ è chiara per la riflessività della relazione di congruenza), possiamo sommare membro a membro usando la (1) del Teorema 3.21 e ottenere

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv_3 a_k + a_{k-1} + \cdots + a_1 + a_0 \quad (3.37)$$

In altre parole, un qualunque n è congruente modulo 3 alla somma delle sue cifre.
Ma allora, poiché n divisibile per 3 significa che n è congruente a 0 modulo 3, si ha che n è divisibile per 3 se e solamente se la somma delle sue cifre è congruente a zero modulo 3, ovvero anche lei divisibile per 3. Il criterio è dimostrato.

Lo stesso identico criterio vale per la divisibilità per 9: il motivo è che si ha anche $10 \equiv_9 1$, quindi si può rifare la stessa dimostrazione da questo punto di partenza.

Ora, vediamo come il Teorema 3.21 ci consenta di definire una somma e una moltiplicazione sull'insieme $\mathbb{Z}_n$ delle classi di congruenza modulo n: questo ci consentirà di fare calcoli su questo insieme, e sviluppare quella che si chiama *aritmetica modulare*.
Piú precisamente, date due classi $[i]$ e $[j]$ della congruenza modulo n, definiamo la loro somma come

$$[i] + [j] := [i + j] \quad (3.38)$$

e il loro prodotto come

$$[i] \cdot [j] := [ij]. \quad (3.39)$$

Il problema di tali definizioni è che definire la somma o il prodotto tra due classi mediante la somma o il prodotto dei rappresentanti i e j potrebbe essere ambiguo: infatti, una stessa classe può essere rappresentata da interi diversi (ad esempio, modulo 3 si ha $[1] = [4]$), quindi dobbiamo assicurarci che anche scegliendo rappresentanti diversi i' e j' per le classi $[i]$ e $[j]$ rispettivamente,

la somma e il prodotto definiti da (3.38) e (3.39) danno sempre lo stesso risultato (ovvero la stessa classe).
Ma questo è garantito proprio dal Teorema 3.21 : infatti, supponiamo che sia $[i'] = [i]$ e $[j'] = [j]$: questo significa che $i \equiv_n i'$ e $j \equiv_n j'$. Ma allora, applicando la (1) del Teorema 3.21 si ha $i+j \equiv_n i'+j'$, ovvero $[i+j] = [i'+j']$: la somma che abbiamo definito non dipende dai rappresentanti scelti per le classi da sommare, e non c'è ambiguità.
Analogamente, sempre supponendo che sia $[i'] = [i]$ e $[j'] = [j]$, ovvero $i \equiv_n i'$ e $j \equiv_n j'$, applicando la (2) del Teorema 3.21 si ha $ij \equiv_n i'j'$, ovvero $[ij] = [i'j']$: anche il prodotto per come lo abbiamo definito non dipende dai rappresentanti scelti per le classi da sommare, e non c'è ambiguità.

A questo punto, come abbiamo fatto ogni volta che ci siamo trovati in presenza di un insieme con una o più operazioni, verifichiamo quali proprietà soddisfano queste operazioni:

(1) La somma è associativa:

$$([i] + [j]) + [k] = [i + j] + [k] = [(i + j) + k] =$$

(sfruttando l'associatività della somma usuale tra gli interi i, j, k)

$$[i + (j + k)] = [i] + [j + k] = [i] + ([j] + [k])$$

(2) la somma è commutativa:

$$[i] + [j] = [i + j] = [j + i] = [j] + [i]$$

dove nell'uguaglianza centrale abbiamo sfruttato il fatto che la somma usuale tra interi è commutativa.

(3) esiste un elemento neutro per la somma, che è la classe $[0]$ di 0:

$$[i] + [0] = [i + 0] = [i]$$

e chiaramente nello stesso modo (o sfruttando il fatto che la somma è commutativa), $[0] + [i] = [i]$.

Si noti che, dal momento che $[0] = [kn]$ per ogni multiplo kn di n, possiamo anche scrivere $[i]+[kn] = [i]$ o, equivalentemente, $i+kn \equiv_n i$: in altre parole, modulo n, ogni intero del tipo kn equivale allo 0.

(4) per ogni classe $[i]$ esiste un inverso per la somma (ovvero un opposto), dato dalla classe $[-i]$:

$$[i] + [-i] = [i + (-i)] = [0].$$

Si noti che se stiamo lavorando modulo n con le classi $[0], [1], \ldots, [n-1]$, e preferiamo vedere ogni classe rappresentata da un numero compreso tra 0 e $n-1$, allora possiamo anche rappresentare l'opposto di $[i]$ come $[n-i]$ in quanto chiaramente $-i \equiv_n n-i$. Ad esempio, in $\mathbb{Z}_5$ l'opposta della classe $[2]$ è certamente $[-2]$, che può essere anche espressa come $[5-2] = [3]$ (e infatti $[2]+[3] = [5] = [0]$).

(5) Il prodotto è associativo:

$$([i][j])[k] = [ij][k] = [(ij)k] =$$

(sfruttando l'associatività del prodotto usuale tra gli interi i, j, k)

$$[i(jk)] = [i][jk] = [i]([j][k])$$

(6) il prodotto è commutativo:

$$[i][j] = [ij] = [ji] = [j][i]$$

dove nell'uguaglianza centrale abbiamo sfruttato il fatto che il prodotto usuale tra interi è commutativo.

(7) esiste un elemento neutro per il prodotto, che è la classe $[1]$ di 1:

$$[i][1] = [i \cdot 1] = [i]$$

e chiaramente nello stesso modo (o sfruttando il fatto che il prodotto è commutativo), $[1][i] = [i]$.

(8) il prodotto è distributivo rispetto alla somma:

$$[i]([j]+[k]) = [i][j+k] = [i(j+k)] = [ij+ik] = [ij]+[ik] = [i][j]+[i][k]$$

e analogamente si mostra che $([i]+[j])[k] = [i][j]+[i][k]$.

Le proprietà appena elencate di dicono che $\mathbb{Z}_n$, dotato delle operazioni di somma e prodotto definite dalle (3.38) e (3.39), è un anello commutativo (Osservazione 3.1).
Tuttavia, rispetto all'anello $\mathbb{Z}$ degli interi, $\mathbb{Z}_n$ presenta alcune importanti differenze: la prima, più evidente, è che si tratta di un anello finito, diversamente da $\mathbb{Z}$ che è infinito.
La seconda importante differenza tra $\mathbb{Z}$ e $\mathbb{Z}_n$ è che in quest'ultimo non vale in generale la legge di annullamento del prodotto (che afferma che un prodotto

è zero solo se almeno uno dei due fattori è nullo): ad esempio, in $\mathbb{Z}_6$ consideriamo le classi [2] e [3]: nessuna di queste due è la classe nulla (ovvero $[2] \neq [0]$ e $[3] \neq [0]$) in quanto né 2 né 3 sono congruenti a zero modulo 6: tuttavia

$$[2][3] = [2 \cdot 3] = [6] = [0]$$

ovvero il loro prodotto è zero.

Un'altra questione fondamentale nell'aritmetica di $\mathbb{Z}_n$ riguarda l'esistenza dell'inverso moltiplicativo di una classe $[i]$ data: nell'anello degli interi $\mathbb{Z}$ sappiamo che gli unici interi x ad avere un inverso moltiplicativo (ovvero un elemento y per cui $xy = yx = 1$) sono $+1$ e -1. Vediamo ora che in $\mathbb{Z}_n$ la questione è leggermente più complessa.

Infatti, sia $[i]$ una classe in $\mathbb{Z}_n$: dire che esiste un inverso moltiplicativo di $[i]$ equivale a dire che esiste un classe $[x]$ tale che $[i][x] = [1]$. Ma quest'ultima uguaglianza , per definizione di prodotto tra classi, significa $[ix] = [1]$ ovvero che ix e 1 sono congrui modulo n, quindi la loro differenza è un multiplo di n:

$$ix - 1 = yn$$

(per un certo intero $y \in \mathbb{Z}$).

Portando yn a primo membro e -1 a secondo, concludiamo che la classe di i ha inverso modulo n se e solo esistono due interi x, y tali che

$$ix - yn = 1 \tag{3.40}$$

e in tal caso l'inverso di $[i]$ è dato proprio dalla classe $[x]$.

Ora, la relazione (3.40), come sappiamo dalla Proposizione 3.16, è verificata sicuramente se il massimo comune divisore di i e n è 1; viceversa, se vale tale relazione allora necessariamente il massimo comune divisore di i e n è 1, perché se d è un divisore comune di i e n (ovvero $i = di'$ e $n = dn'$) allora sostituendo nella (3.40) otteniamo

$$ix - yn = di'x - ydn' = d(i'x - yn') = 1$$

che ci dice che necessariamente $d = \pm 1$ (diversamente, non esiste nessun intero che moltiplicato per d dà 1).

In altre parole, abbiamo appena dimostrato che *una classe $[i]$ in $\mathbb{Z}_n$ è invertibile se e solo se il massimo comune divisore di i e n è 1, ovvero se e solo se i e n sono primi tra loro.*

Quanto detto sopra per ottenere questo risultato ci fornisce anche un modo pratico per il calcolo dell'inverso, quando questo esiste. Ad esempio, determiniamo l'inverso di [5] in $\mathbb{Z}_{14}$ (o, detto in altre parole, l'inverso di 5 modulo 14).

Innanzitutto, tale inverso esiste perché 5 e 14 sono primi tra loro: per trovare tale inverso, ovvero l'intero x per cui è soddisfatta la (3.40), eseguiamo il procedimento di divisioni successive visto nel paragrafo precedente:

$$14 = 5 \cdot 2 + 4$$
$$5 = 4 \cdot 1 + 1$$
$$4 = 1 \cdot 4$$

Dalla seconda divisione troviamo $1 = 5 - 4$, e sostituendo 4 tramite $4 = 14 - 5 \cdot 2$ (ricavata dalla prima divisione) otteniamo

$$1 = 5 - 4 = 5 - (14 - 5 \cdot 2) = 5 - 14 + 5 \cdot 2 = 5 \cdot 3 + (-1) \cdot 14$$

Quindi, in base a quanto visto sopra, 3 è l'inverso di 5 modulo 14, ovvero [3] è l'inverso di [5] in $\mathbb{Z}_{14}$ (infatti, $[5][3] = [15] = [1]$ in $\mathbb{Z}_{14}$).

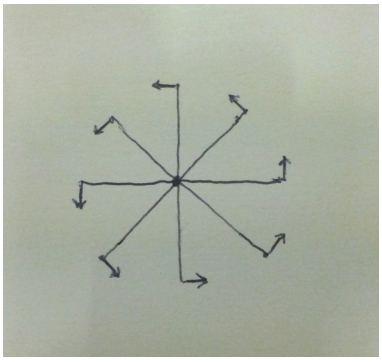
Come corollario di quanto appena detto, notiamo che se n è un numero primo, allora per ogni $i = 1, 2, \ldots, n-1$ si ha che i è primo con n, quindi in $\mathbb{Z}_n$ le classi $[1], [2], \ldots, [n-1]$ (cioè tutte le classi tranne la classe nulla [0]) ammettono un inverso: questo, in base alla definizione data nell'Osservazione 3.1 ci dice che *se n è primo allora $\mathbb{Z}_n$ è un campo* (esattamente come $\mathbb{Q}$ e $\mathbb{R}$). In particolare, in $\mathbb{Z}_n$ con n primo, come in tutti i campi, vale la legge di annullamento del prodotto[5]

Osservazione 3.22. Le proprietà (1), (2), (3) e (4) dell'operazione di somma tra classi che abbiamo visto sopra ci dicono che $\mathbb{Z}_n$, rispetto a tale operazione, è un gruppo commutativo (Definizione 2.30).

Una interessante "realizzazione geometrica" di questo gruppo può essere data come segue: consideriamo il gruppo delle simmetrie della seguente figura del piano[6], una sorta di girandola con tutti i bracci della stessa lunghezza, ottenuta dividendo l'angolo giro di $360° = 2\pi$ in 8 parti uguali.

[5]Infatti, siano a e b elementi di un campo tali che $ab = 0$ e supponiamo per assurdo che a e b siano entrambi diversi da zero: allora, moltiplicando entrambi i membri di $ab = 0$ per l'inverso a^{-1} di a si ottiene da una parte $a^{-1}(ab) = a^{-1}0 = 0$, dall'altra $a^{-1}(ab) = (a^{-1}a)b = 1b = b$, ovvero $b = 0$, contro l'ipotesi che a e b fossero entrambi non nulli.

[6]Ricordiamo che le simmetrie di una figura sono i movimenti rigidi (traslazioni, rotazioni, riflessioni) che la lasciano invariata, rispetto all'operazione di composizione.

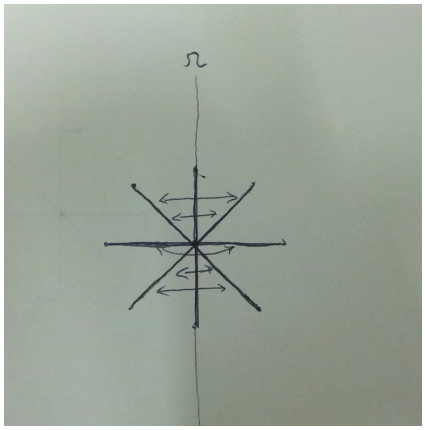


Sicuramente la rotazione di angolo $\frac{2\pi}{8} = 45°$ in senso antiorario lascia invariata la figura (comprese le freccette che spuntano da ogni braccio), così come la rotazione di $\frac{2\pi}{8} \cdot 2 = 90°$ (ottenuta componendo la rotazione di 45° con se stessa), la rotazione di $\frac{2\pi}{8} \cdot 3 = 135°$ (ottenuta componendo la rotazione di 45° con se stessa 3 volte) e così via tutte le rotazioni di angolo $\frac{2\pi}{8} \cdot k$, ottenute componendo k volte la rotazione di 45°.
Tuttavia, è chiaro che se considero la rotazione di angolo $\frac{2\pi}{8} \cdot 8$, ottengo esattamente la funzione identica che manda ogni punto in se stesso (8 rotazioni di 45° una dietro l'altra danno un giro completo), e la stessa cosa sarà vera se ruoto di $\frac{2\pi}{8} \cdot 16$, $\frac{2\pi}{8} \cdot 24$ e in generale per qualunque multiplo di 8; analogamente, una rotazione di $\frac{2\pi}{8} = 45°$ muove i punti nello stesso modo di una rotazione di $\frac{2\pi}{8} \cdot 9$ (un giro completo più altri 45°), o di $\frac{2\pi}{8} \cdot 17$ (due giri completi più altri 45°) e così via per tutte le rotazioni di $\frac{2\pi}{8} \cdot k$ con k che differisce da 1 per un multiplo di 8.
In generale, avremo che un angolo di $\frac{2\pi}{8} \cdot k$ e un angolo di $\frac{2\pi}{8} \cdot l$ rappresentano la stessa rotazione se e solo se k e l differiscono per un multiplo di 8: ma questa è esattamente la relazione di congruenza modulo 8 che definisce le classi di $\mathbb{Z}_8$.
Quindi c'è una corrispondenza biunivoca tra le classi $\{[0], [1], [2], [3], [4], [5], [6], [7]\}$ e le rotazioni che lasciano invariata la figura: alla classe $[k]$ corrisponde la rotazione di angolo $\frac{2\pi}{8} \cdot k$, e chiaramente $[k] = [k']$ se e solo se la rotazione di $\frac{2\pi}{8} \cdot k$ coincide con la rotazione di $\frac{2\pi}{8} \cdot k'$ (visto che k e k' differiscono per un multiplo di 8).
Questa corrispondenza identifica il gruppo $\mathbb{Z}_n$ con il gruppo delle simmetrie della figura non solo come insiemi, ma anche rispetto alle operazioni in ciascuno dei due: se compongo due rotazioni di angoli $\frac{2\pi}{8} \cdot k$ e $\frac{2\pi}{8} \cdot l$ (che corrispondono alle classi $[k]$ e $[l]$ in $\mathbb{Z}_n$), il risultato sarà la rotazione di $\frac{2\pi}{8} \cdot k + \frac{2\pi}{8} \cdot l = \frac{2\pi}{8} \cdot (k + l)$, che corrisponde alla classe $[k + l]$: quindi la composizione in un gruppo corrisponde esattamente alla somma nell'altro, e così vengono preservate anche tutte le altre relazioni: ad esempio, il fatto che

in $\mathbb{Z}_8$ si abbia $[5]+[3]=[0]$ (piú precisamente, $[5]+[3]=[5+3]=[8]=[0]$) corrisponde nel gruppo delle simmetrie della figura al fatto che se compongo una rotazione di $\frac{2\pi}{8}\cdot 5$ con una di $\frac{2\pi}{8}\cdot 3$ ottengo l'identità (l'elemento neutro per la composizione), in quanto avrò fatto un giro completo.

Quando tra due gruppi esiste una corrispondenza biunivoca tale che le operazioni che faccio nel primo gruppo corrispondono nel senso descritto sopra alle operazioni che faccio nel secondo, si dice che *i due gruppi sono isomorfi*. In pratica, se due gruppi sono isomorfi possiamo considerarli come se fossero lo stesso gruppo, anche se sono di natura molto diversa tra loro come nel nostro esempio (il primo è costituito di classi di numeri interi e l'operazione è una somma, il secondo da trasformazioni geometriche e l'operazione è la composizione).

Per concludere, si noti che le freccette nella figura servono a far sì che le rotazioni siano le sue *uniche* simmetrie, così da poterle identificare con gli elementi di $\mathbb{Z}_8$; se non avessimo messo le freccette, ci sarebbero state altre simmetrie (ad esempio le riflessioni rispetto alle rette che contengono i bracci) e tale identificazione non sarebbe stata possibile:



Abbiamo visto che trovare l'inverso di un intero a modulo n (cioè un x tale che $[a][x]=[1]$, ovvero $[ax]=[1]$) equivale a risolvere l'equazione

$$ax \equiv_n 1.$$

Affrontiamo ora il problema più generale di determinare le soluzioni dell'equazione

$$ax \equiv_n b \tag{3.41}$$

dove b è un qualunque numero intero. Le domande a cui vogliamo rispondere sono: quando questa equazione è risolubile? se sì, quali e quante sono le sue soluzioni?
La risposta alla prima domanda ci è fornita dal seguente

Teorema 3.23. L'equazione $ax \equiv_n b$ ammette soluzioni se e solo se il massimo comune divisore d di a e n divide b.

Proof. Mostriamo prima che se il massimo comune divisore $d = (a, n)$ divide b, allora l'equazione ha soluzioni: come sappiamo, se d è il massimo comune divisore di a e n, esistono due interi t e s tali che

$$d = at + ns \tag{3.42}$$

Ora, l'ipotesi che d divida b significa che $b = db'$ per qualche intero b': moltiplicando allora la (3.42) a entrambi i membri proprio per b' si ottiene

$$b = db' = atb' + nsb' \tag{3.43}$$

Ma quest'ultima uguaglianza ci dice che atb' è uguale a b modulo n (perché differisce da b per nsb', che è un multiplo di n), ovvero $atb' \equiv_n b$: allora $x = tb'$ è una soluzione di $ax \equiv_n b$. Quindi, come volevamo, abbiamo mostrato che l'equazione ammette soluzioni sotto l'ipotesi che il massimo comune divisore di a e n divida b.
Viceversa, supponiamo che l'equazione $ax \equiv_n b$ ammetta soluzioni: questo significa che esiste un intero x_0 tale che b e ax_0 differiscono solo per un multiplo di n, ovvero

$$b = ax_0 + ny \tag{3.44}$$

per qualche $y \in \mathbb{Z}$. Ma da questa uguaglianza è facile mostrare che il massimo comune divisore d di a e n divide b: infatti, essendo d un divisore comune di a e n si ha che $a = da'$ e $n = dn'$ per certi interi a', n', e sostituendo queste due uguaglianze nella (3.44) si trova subito

$$b = da'x_0 + dn'y = d(a'x_0 + n + y)$$

che ci dice proprio che d divide b. □

La dimostrazione appena fatta, oltre a darci il criterio necessario e sufficiente perché l'equazione $ax \equiv_n b$ sia risolubile, in caso affermativo ci suggerisce anche come trovare almeno una soluzione. Vediamo subito un esempio: supponiamo di voler risolvere l'equazione

$$12x \equiv_{39} 15.$$

Poiché il massimo comune divisore tra $a = 12$ e $n = 39$ è $d = 3$, e 3 divide $b = 15$, il Teorema 3.23 ci dice che esiste almeno una soluzione. Per trovarla, seguiamo passo passo la dimostrazione: esprimiamo prima $d = 3$ come combinazione di $n = 39$ e $a = 12$ come fatto nella (3.42), tramite il metodo delle divisioni successive:

$$39 = 12 \cdot 3 + 3$$

$$12 = 3 \cdot 4$$

Le divisioni confermano che il massimo comune divisore di 12 e 39 è 3, in quanto è l'ultimo resto non nullo, e dalla prima divisione otteniamo $3 = 39 - 12 \cdot 3$, ovvero

$$3 = 12 \cdot (-3) + 39 \cdot 1 \tag{3.45}$$

che sarebbe la (3.42) con $t = -3$ e $s = 1$. Ora, esattamente come fatto nella dimostrazione, osserviamo che $b = 15 = 3 \cdot 5$ (cioè, sempre in riferimento alla dimostrazione, sarebbe $b' = 5$) e moltiplichiamo la (3.45) proprio per 5, ottenendo

$$15 = 3 \cdot 5 = 12 \cdot (-3) \cdot 5 + 39 \cdot 5 = 12 \cdot (-15) + 39 \cdot 5 \tag{3.46}$$

Ma allora $x_0 = -15$ è una soluzione dell'equazione: infatti, la (3.46) ci dice proprio che $12 \cdot (-15)$ è uguale a 15 modulo 39 (essi differiscono per $39 \cdot 5$).

Quella che abbiamo trovato è solo una soluzione dell'equazione: ce ne sono altre? La risposta ce la dà il seguente risultato, di cui omettiamo la dimostrazione.

Teorema 3.24. Se l'equazione $ax \equiv_n b$ ha soluzioni, esse si ottengono tutte sommando a una qualunque di esse x_0 i multipli di $\frac{n}{d}$ (ovvero $x = x_0 + \frac{n}{d}k$, per ogni $k \in \mathbb{Z}$), dove d è il massimo comune divisore di a e n.

Per illustrare il teorema, applichiamolo all'equazione $12x \equiv_{39} 15$, di cui sopra abbiamo trovato una soluzione $x_0 = -15$.
Poiché in quel caso $n = 39$ e $d = 3$, abbiamo che le soluzioni sono tutti e soli gli interi del tipo

$$x = x_0 + k\frac{n}{d} = -15 + \frac{39}{3}k = -15 + 13k$$

Queste, al variare di $k \in \mathbb{Z}$, sono tutte le soluzioni dell'equazione $12x \equiv_{39} 15$, che quindi risulta avere infinite soluzioni in $\mathbb{Z}$.
Per comprendere meglio la struttura dell'insieme delle soluzioni, distinguiamo però nell'espressione generale della soluzione $x = -15 + 13k$ tre casi:

(1) k è un multiplo di 3, ovvero $k = 3k'$ per qualche $k' \in \mathbb{Z}$.

In tal caso le soluzioni sono

$$x = -15 + 13k = -15 + 13 \cdot 3k' = -15 + 39k'$$

Questo ci dice che quando k è multiplo di 3 le soluzioni che otteniamo, pur essendo interi diversi, sono tutte equivalenti modulo 39, ovvero stanno tutte nella classe $[-15]$ di -15.

(2) k è un intero del tipo $k = 3k' + 1$ per qualche $k' \in \mathbb{Z}$.

In tal caso le soluzioni sono

$$x = -15 + 13k = -15 + 13 \cdot (3k' + 1) = -15 + 39k' + 13 = -2 + 39k'$$

Di nuovo otteniamo una famiglia di soluzioni che sono tutte equivalenti modulo 39, e più precisamente tutte congruenti a -2. Esse formano la classe $[-2]$ di -2 modulo 39 che, si noti, è diversa in $\mathbb{Z}_{39}$ dalla classe ottenuta nel caso (1) (infatti, $[-15] \neq [-2]$ in quanto la differenza $-15 - (-2) = -13$ non è un multiplo di 39)

(3) k è un intero del tipo $k = 3k' + 2$ per qualche $k' \in \mathbb{Z}$.

In tal caso le soluzioni sono

$$x = -15 + 13k = -15 + 13 \cdot (3k' + 2) = -15 + 39k' + 26 = 11 + 39k'$$

Ancora, otteniamo una famiglia di soluzioni che sono tutte equivalenti modulo 39, e più precisamente tutte congruenti a 11. Esse formano la classe $[11]$ di 11 modulo 39 che, si noti, è diversa in $\mathbb{Z}_{39}$ da entrambe le classi ottenute nei casi (1) e (2) (infatti, $[11] \neq [-2]$ e $[11] \neq [-15]$ in quanto nessuna delle due differenze $11 - (-2) = 13$ e $11 - (-15) = 26$ è un multiplo di 39)

Si noti che non abbiamo altri casi: le uniche possibilità quando dividiamo k per 3 è che il resto sia $0, 1$ o 2, che corrispondono rispettivamente ai tre casi considerati $k = 3k'$, $k = 3k' + 1$ o $k = 3k' + 2$.

Possiamo riassumere quanto appena visto come segue: l'equazione $12x \equiv_{39} 15$ ha infinite soluzioni se la consideriamo come un'equazione da risolvere in $\mathbb{Z}$, ma se la pensiamo come l'equazione $[12][x] = [15]$ (infatti, dire $12x \equiv_{39} 15$

significa $[12x] = [15]$, ovvero per definizione di prodotto tra classi proprio $[12][x] = [15]$) da risolvere in $\mathbb{Z}_{39}$, essa ha esattamente tre soluzioni distinte: $[-15], [-2], [11]$.

Aiutati da questo esempio, possiamo allora dire che, in generale, *se l'equazione* $ax \equiv_n b$ *ha soluzioni, ovvero se il massimo comune divisore* d *di* a *e* n *divide* b*, allora queste soluzioni sono esattamente* d *modulo* n.
In particolare, *se* a *e* n *sono primi tra loro, ovvero il loro massimo comune divisore* d *è* 1*, allora la soluzione esiste per ogni* b *ed è unica (modulo* n*).*
Questo è in accordo con il fatto che se a e n sono primi tra loro, allora a ammette un inverso moltiplicativo modulo n, che possiamo denotare a^{-1}, quindi l'equazione $ax \equiv_n b$ può essere semplicemente risolta (cioè, x può essere determinato in modo unico modulo n) semplicemente moltiplicando entrambi i membri per a^{-1}:

$$ax \equiv_n b \Rightarrow a^{-1}(ax) \equiv_n a^{-1}b \Rightarrow (a^{-1}a)x \equiv_n a^{-1}b \Rightarrow 1x \equiv_n a^{-1}b \Rightarrow x \equiv_n a^{-1}b$$

In altre parole, se esiste l'inverso di a la soluzione può essere trovata esattamente come si risolve normalmente l'equazione $ax = b$ nei reali o nei razionali.

3.4 Applicazioni: cenni alla crittografia e ai numeri casuali

Vedremo adesso alcune importanti applicazioni pratiche dell'aritmetica modulare e dei teoremi visti nel capitolo precedente.
La prima di tali applicazioni riguarda la crittografia, ovvero lo studio delle tecniche con le quali un mittente può spedire un messaggio a un destinatario criptandolo, ovvero rendendolo illeggibile a tutti tranne al destinatario che deve essere l'unico a conoscere il modo di decriptarlo.

Per capire in che modo l'aritmetica modulare possa entrare in questo discorso, supponiamo di voler criptare un messaggio scritto con le 21 lettere dell'alfabeto italiano

$$A, B, C, D, \ldots, T, U, V, Z.$$

Un modo per farlo può essere quello di far corrispondere a ogni lettera dell'alfabeto un'altra lettera e poi sostituire le lettere che compaiono nel messaggio dato in base alla corrispondenza scelta.
Se ad esempio la corrispondenza che scegliamo è tale che manda A in P, D in V, T in L , la parola DATA verrà trasformata nella parola $VPLP$.

Il destinatario, per decriptare tale messaggio, deve essere a conoscenza della corrispondenza scelta e deve riapplicarla a ritroso per riottenere il messaggio.
Chiaramente, quella che stiamo chiamando corrispondenza tra le lettere dell'alfabeto deve essere più precisamente una corrispondenza biunivoca di tali lettere, ovvero una funzione biiettiva tra l'alfabeto e se stesso (in altre parole, una permutazione delle lettere dell'alfabeto): infatti, se la corrispondenza non fosse iniettiva, cioè se per esempio mandassimo A in P e anche O in P, il destinatario leggendo $VPLP$ non saprebbe se al posto della P deve sostituire una A o una O, e non saprebbe se il messaggio originale era per esempio $DATA$, $DATO$, $DOTO$ etc.
Quindi, una qualunque permutazione realizza una cifratura del messaggio, e la decifratura si realizza applicando la permutazione inversa (che esiste ben definita perché una permutazione è una funzione biiettiva, ovvero invertibile).
Ora, tra tutte le permutazioni del nostro insieme di 21 elementi può essere conveniente (per comodità di comunicazione con il destinatario) scegliere quelle che possono essere descritte senza dover per forza dare il corrispondente di ogni lettera ma tramite una qualche regola.
Ad esempio, è noto che Cesare per cifrare i suoi messaggi usava la permutazione che si ottiene associando a ogni lettera quella che si trova 3 posizioni più avanti nell'alfabeto: più precisamente, alla A associa la D, alla B la E, e così via, fino alla T, a cui verrà associata la Z, che è l'ultima lettera dell'alfabeto, e a quel punto per le ultime tre lettere si riparte da capo: alla U associo la A, alla V la B e alla Z la C.
Nel linguaggio del gruppo delle permutazioni imparato nel capitolo precedente, la permutazione usata da Cesare non è nient'altro che il prodotto di tre cicli disgiunti, ciascuno di lunghezza 7.

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

Benché fino a questo punto l'oggetto matematico che più si presta allo studio dei cifrari sembrino essere le permutazioni, vediamo ora che il modo più semplice di scrivere la corrispondenza di Cesare si ottiene proprio usando il linguaggio delle congruenze.
A questo scopo, iniziamo con il tradurre numericamente l'alfabeto, assegnando a ogni lettera il numero della sua posizione nell'alfabeto stesso: la A sarà quindi rappresentata dal numero 1, la B dal numero 2 e così via fino alla Z che sarà rappresentata dal numero 21.
Allora, la regola stabilita da Cesare per il suo cifrario dovrebbe essere semplicemente

$$x \mapsto x + 3$$

cioè alla lettera corrispondente al numero x associamo la lettera che corrisponde alla posizione $x+3$ (ad 1, cioè A, corrisponde $1+3=4$, cioè D, e così via).
Tuttavia, la formula sembra funzionare solo fino a $x = 18$ (ovvero T) a cui viene associata come abbiamo detto sopra $x+3=21$ (ovvero la Z), dal momento che per $x = 19$ (cioè la U) abbiamo $x+3 = 22$, che non corrisponde a nessuna lettera dell'alfabeto: ma in realtà il problema si risolve se lavoriamo invece che nell'aritmetica usuale degli interi nell'aritmetica modulo 21, in quanto 22 corrisponde a 1 (ovvero alla A) modulo 21, e infatti il cifrario di Cesare prevede di associare alla U la A: analogamente, a $x = 20$ (cioè la V) corrisponde $x+3 = 23$ che è congruo a 2 (ovvero la B) modulo 21 e a $x = 21$ (cioè la Z) corrisponde $x+3 = 24$ che è congruo a 3 (ovvero la C) modulo 21.
Quindi la formula che descrive correttamente il cifrario di Cesare è

$$x \mapsto x + 3 \ (mod\ 21) \tag{3.47}$$

Il fatto che il cifrario di Cesare sia un procedimento crittografico corretto, cioè una funzione biiettiva sull'insieme delle lettere dell'alfabeto (deve esserlo per poter essere invertita dal destinatario che deve decifrare il messaggio), equivale al fatto che la (3.47) è una funzione biiettiva sull'insieme $\mathbb{Z}_{21} = \{1, 2, \ldots, 21\}$ (per comodità di notazione stiamo omettendo le parentesi quadre nell'indicare le classi).
Infatti, la biiettività della (3.47) si vede dal fatto che se $x + 3 \equiv y \ (mod\ 21)$ allora x si può riottenere in modo unico da y semplicemente risolvendo l'equazione, il che in questo caso si fa semplicemente portando il 3 a secondo membro: $x \equiv y - 3 \ (mod\ 21)$ (equivalentemente, essendo -3 congruo a $21 - 3 = 18$ modulo 21, potremo scrivere $x = y + 18 \ (mod\ 21)$: ad esempio se $y = 4$, che corrisponde alla D, decriptando abbiamo $x = y + 18 = 22$ che è congruo a 1 modulo 21, ovvero la A).

A questo punto, ispirati da questo, possiamo pensare di realizzare nuovi cifrari semplicemente sostituendo al posto di $x + 3$ una qualunque funzione $f(x)$ purché questa sia invertibile in $\mathbb{Z}_{21}$: come primo facile esempio, possiamo considerare, per ogni b, la generalizzazione del cifrario di Cesare

$$x \mapsto x + b \ (mod\ 21) \tag{3.48}$$

che corrisponde a associare a ogni lettera che si trova nella posizione x dell'alfabeto la lettera che si trova b posizioni più avanti (se $b > 0$) o più indietro (se $b < 0$).

L'invertibilità di tale funzione si mostra esattamente come fatto per il cifrario di Cesare, ovvero basta osservare che, per ogni y, l'equazione $x + b \equiv y \ (mod\ 21)$ ha unica soluzione data da $x \equiv y - b \ (mod\ 21)$

Un ulteriore passo avanti nella generalizzazione del cifrario di Cesare si ottiene come segue:

$$x \mapsto ax + b \ (mod\ 21) \tag{3.49}$$

Ad esempio, se $a = 5$ e $b = 3$, allora la lettera D, che corrisponde a $x = 4$, viene mandata in $5x + 3 = 23 \ (mod\ 21)$ ovvero $2 \ (mod\ 21)$, che corrisponde alla lettera B.

Stavolta, però, dobbiamo fare più attenzione, in quanto non ogni scelta di a ci dà un procedimento crittografico corretto: infatti, come abbiamo detto sopra, la funzione (3.49) deve essere biiettiva, e questo corrisponde a dire che per ogni y l'equazione $ax + b \equiv y \ (mod\ 21)$ deve avere soluzione e questa deve essere unica.

Ora, portando b a secondo membro questo equivale a dire che deve essere unica la soluzione di $ax \equiv y - b \ (mod\ 21)$.

Ma alla fine del paragrafo precedente abbiamo visto qual è la condizione per l'unicità di tale soluzione: a deve essere primo con 21. Questo infatti garantisce che a abbia un inverso a^{-1} modulo 21 e quindi, come abbiamo visto nel paragrafo precedente, la soluzione si ottiene moltiplicando entrambi i membri per a^{-1}:

$$x \equiv a^{-1}(y - b) \ (mod\ 21)$$

che è la formula per decriptare il messaggio criptato.

Il cifrario dato dalla (3.49) si chiama *cifrario affine*.

Esempio 3.25. Supponiamo, sbagliando, di voler criptare un messaggio con la regola $x \mapsto 6x \ (mod\ 21)$ (l'errore consiste nel fatto che si tratta di una formula del tipo (3.49) con $b = 0$ e $a = 6$ non primo con $n = 21$).

Allora, vediamo ad esempio che 1 (cioè la A) viene mandato in 6 (cioè F); ma anche H, che corrisponde a 8, viene mandato in $6x = 48 \equiv 6 \ (mod\ 21)$, ovvero nuovamente la F.

Tale metodo di cifratura non è quindi corretto in quanto si hanno lettere diverse mandate nella stessa lettera, e il messaggio criptato sarebbe ambiguo.

Un fatto fondamentale quando si trasmette un messaggio criptato è che ovviamente si vuole che questo sia il più possibile difficile da decriptare per chi, non essendo il destinatario, lo intercettasse.

Ora, per decriptare un messaggio bisogna innanzittutto conoscere la funzione $x \mapsto f(x)$ con cui si cripta il messaggio, e poi saper calcolare l'inversa di tale funzione.
Per quello che riguarda la conoscenza della funzione f, supponendo che chi intercetta il messaggio sappia di che tipo di cifrario si tratta, ad esempio un cifrario affine (3.49), questi dovrebbe conoscere la coppia (a, b) per sapere esattamente chi è la funzione e invertirla.
Tale coppia, e più in generale i parametri che servono per costruire la funzione con cui criptiamo il messaggio, si chiama la *chiave del cifrario*.
Chiaramente, più sono le chiavi possibili di un tipo di cifrario, più sarà difficile per chi lo intercetta di determinarle: ad esempio, il cifrario di Cesare generalizzato $x \mapsto x + b \ (mod\ 21)$ ha come chiave la b: questa può essere scelta esattamente in 21 modi ($b = 1, 2, \ldots, 21$), ma escludendo $b = 21$ con il quale assoceremmo a ogni lettera se stessa, otteniamo 20 cifrari diversi.
Nel caso del cifrario affine (3.49), abbiamo che b può variare tra 1 e 21 mentre come a possiamo scegliere un qualunque intero positivo minore di 21 e primo con esso: ma il numero di interi positivi minori di 21 e primi con esso è dato, come abbiamo visto nel paragrafo precedente, da $\phi(21)$, dove ϕ è la funzione di Eulero. Essendo $21 = 3 \cdot 7$, in base alla formula (3.35) abbiamo $\phi(21) = 21(1 - 1/3)(1 - 1/7) = 12$.
Quindi per un cifrario affine, tenendo conto che per ognuna delle 12 scelte di a abbiamo 20 scelte possibili di b, abbiamo $12 \cdot 21 = 252$ possibili chiavi, dalle quali escludiamo però il caso $a = 1, b = 21$, che, essendo 21 congruente a 0 modulo 21, manda ogni numero in stesso. Quindi, chiunque sia interessato a decriptare il messaggio, sospettando che si tratti di un cifrario affine, potrebbe doverle provare tutte (il che chiaramente non è troppo complicato con i computer a disposizione oggi).

Il secondo aspetto della sicurezza di un codice, come abbiamo detto, riguarda la difficoltà di calcolare la funzione inversa di quella usata per la cifratura: a prima vista, sembrerebbe che una volta nota la chiave, ovvero la funzione f, calcolare l'inversa di f sia una cosa relativamente semplice. In realtà stiamo per mostrare un codice, detto RSA, nella quale il calcolo della funzione inversa si rivela talmente complesso che anche conoscendo in che modo il messaggio è stato criptato e conoscendo la chiave, in assenza di altre informazioni la decifratura risulta praticamente impossibile: si tratta di un esempio di cosiddetta *crittografia a chiave pubblica* e più precisamente la cosiddetta RSA (dalle iniziali dei nomi Rivest, Shamir e Adleman che l'hanno introdotta nel 1977).
Vediamo i dettagli: supponiamo che il messaggio che vogliamo trasmettere sia un numero intero x (che può rappresentare una lettera dell'alfabeto ma

anche una qualunque altra informazione).
Il destinatario del messaggio comunica (pubblicamente) al mittente in che modo deve criptare il messaggio, che poi solo lui saprà decriptare invertendo la funzione usata. Più precisamente, il destinatario procede come segue:

(1) sceglie due numeri primi p_1 e p_2 il più grandi possibile e li moltiplica ottenendo $N = p_1 p_2$

(2) calcola la funzione di Eulero $\phi(N)$ (in questo caso si ha $\phi(N) = (p_1 - 1)(p_2 - 1)$)

(3) sceglie un intero positivo $e < \phi(N)$ e che sia primo con $\phi(N)$

(4) comunica al mittente, che vuole spedire l'intero x, di calcolare il valore di $x^e \ (mod\ N)$ e spedirglielo

In altre parole, la funzione di cifratura è $x \mapsto y \equiv x^e \ (mod\ N)$.
Per la correttezza della cifratura, si ha che x deve in realtà essere minore di N, ma tale condizione non è difficile da realizzare soprattutto visto che il destinatario ha ottenuto N moltiplicando due primi molto grandi.
Ora, vediamo che sotto le condizioni date, tale funzione è invertibile ma il calcolo della sua funzione inversa richiede un'informazione in più, oltre alla chiave (N, e) comunicata pubblicamente, che solo il destinatario possiede e che risulta di estrema difficoltà ricavare dalla chiave, anche con l'ausilio di un computer.
Più precisamente, il destinatario che ha ricevuto $y \equiv x^e \ (mod\ N)$ lo decripta come segue: dal momento che e è primo con $\phi(N)$, esso è invertibile modulo $\phi(N)$ e ne calcola il suo inverso, che chiamiamo d. A questo punto, affermiamo che la x può essere ricostruita dalla y tramite la formula

$$x = y^d \ (mod\ N) \tag{3.50}$$

Prima di spiegare il perché, osserviamo che il calcolo di d, che è l'inverso di e modulo $\phi(N)$, richiede la conoscenza della funzione $\phi(N)$, e qui sta esattamente la difficoltà di violare il codice: infatti, tutti conoscono N, che fa parte della chiave pubblica, ma il calcolo di $\phi(N) = (p_1 - 1)(p_2 - 1)$ richiede la conoscenza della decomposizione $N = p_1 p_2$ di N come prodotto di primi, e questo è un calcolo estremamente difficile, per numeri grandi, anche per computer molto potenti.

Ora spieghiamo perché la (3.50) fornisca l'inversa che serve per decifrare il messaggio cifrato: infatti, dal momento che $y \equiv x^e \ (mod\ N)$, elevando entrambi i membri della congruenza alla potenza d si ha

$$y^d \equiv (x^e)^d \equiv x^{ed} \ (mod\ N) \tag{3.51}$$

Quindi, per concludere che $y^d \equiv x \ (mod\ N)$ ci basta mostrare che

$$x^{ed} \equiv x \ (mod\ N) \tag{3.52}$$

Per dimostrare la (3.52) bisogna distinguere due casi: quello in cui x è primo con N e quello in cui x non è primo con N (che può capitare, in quanto noi sappiamo che $x < N$, il che non garantisce che sia non abbia fattori in comune con N). Per semplicità, mostreremo la (3.52) solo nel primo caso.
In tal caso, si sfrutta il seguente cosiddetto *teorema di Eulero*, che non dimostriamo:

Teorema 3.26. Se x e N sono interi primi tra loro, allora

$$x^{\phi(N)} \equiv 1 \ (mod\ N) \tag{3.53}$$

In che modo il teorema di Eulero ci serve per dimostrare la (3.52)?
Per definizione, d è l'inverso di e modulo $\phi(N)$, ovvero $ed \equiv_{\phi(N)} 1$, che in altre parole significa che esiste un intero k per cui $ed = 1 + k\phi(N)$. Ma allora si ha

$$x^{ed} \equiv x^{1+k\phi(N)} \ (mod\ N) \tag{3.54}$$

Ora, in base al teorema di Eulero, $x^{\phi(N)} \equiv 1 \ (mod\ N)$, ovvero, elevando entrambi i membri di tale congruenza alla potenza k si ha

$$x^{k\phi(N)} \equiv (x^{\phi(N)})^k \equiv 1^k \equiv 1 \ (mod\ N) \tag{3.55}$$

ovvero anche $x^{k\phi(N)} \equiv 1 \ (mod\ N)$. Ma allora, moltiplicando entrambi membri di questa uguaglianza per x si ottiene

$$x \cdot x^{k\phi(N)} \equiv x \cdot 1 \ (mod\ N)$$

ovvero

$$x^{1+k\phi(N)} \equiv x \ (mod\ N) \tag{3.56}$$

Combinando la (3.54) e la (3.56) si ha proprio la (3.52), e abbiamo concluso.

Esempio 3.27. Supponiamo di prendere $p_1 = 7$, $p_2 = 5$: allora $N = 35$ e $\phi(N) = (p_1 - 1)(p_2 - 1) = 6 \cdot 4 = 24$. Scegliamo allora $e = 5$ che come previsto è primo con $\phi(N) = 24$.
Supponiamo che il mittente voglia mandare al destinatario il messaggio $x = 3$. Allora, il destinatario gli chiede prima di criptarlo secondo la formula

$x \mapsto x^e \ (mod\ N)$, dopo avergli comunicato pubblicamente la chiave $(N, e) = (35, 5)$. Si ha

$$x^e = 3^5 = 243 \equiv 33 \ (mod\ 35)$$

Il mittente comunica quindi al destinatario il messaggio criptato $y = 33$.
A questo punto, per decriptarlo il destinatario calcola prima l'inverso di $e = 5$ modulo $\phi(N) = 24$. Essendo

$$24 = 5 \cdot 4 + 4$$

$$5 = 4 \cdot 1 + 1$$

$$4 = 4 \cdot 1$$

Dalla seconda divisione troviamo $1 = 5 - 4$, e sostituendo $4 = 24 - 5 \cdot 4$ (ricavato dalla prima) si trova

$$1 = 5 - (24 - 5 \cdot 4) = 5 - 24 + 5 \cdot 4 = -24 + 5 \cdot 5$$

che ci dice che 5 è l'inverso di 5 modulo 24, ovvero $d = 5$.
Allora, il destinatario decripta il messaggio calcolando

$$33^5 = 39.135.393 \equiv 3 \ (mod\ 35)$$

(in quanto $39.135.393 = 35 \cdot 1.118.154 + 3$) e ritrova quindi il messaggio originale $x = 3$

Osservazione 3.28. Se N è un numero primo P, allora sapendo che $\phi(P) = P - 1$ si trova che il teorema di Eulero in questo caso si scrive

$$x^{P-1} \equiv 1 \ (mod\ P) \tag{3.57}$$

(sempre valida sotto l'ipotesi che x sia primo con P).
Questo è quello che si chiama *piccolo teorema di Fermat*.
Moltiplicando entrambi i membri della (3.57) per x si ottiene

$$x^P \equiv x \ (mod\ P) \tag{3.58}$$

che ha il vantaggio di essere vera anche senza ipotesi su x (infatti, se x non è primo con P, essendo P primo, deve essere un multiplo di P, il che implica che sia x^P che x sono congruenti a zero modulo P, e quindi congruenti tra loro). A volte quando si parla di piccolo teorema di Fermat si intende la (3.58).

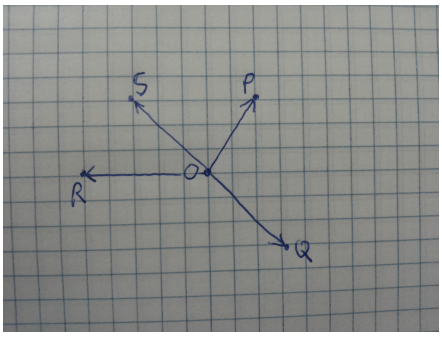
Chapter 4

Vettori, coordinate e geometria

In questo capitolo vedremo come, passando per i cosiddetti vettori geometrici, si possano introdurre nel piano e nello spazio sistemi di coordinate che permettono la traduzione di oggetti e problemi geometrici in oggetti numerici e problemi algebrici: tale costruzione, oltre a essere di fondamentale importanza per le applicazioni alla grafica, ci permetterà di introdurre nozioni basilari della cosiddetta *algebra lineare* che saranno approfondite nei capitoli successivi e che presentano, come vedremo, altre numerose applicazioni in tutte le scienze applicate e in informatica in particolare.

4.1 Vettori geometrici

Un *vettore geometrico applicato nel piano* è un segmento orientato che va da un punto fissato O verso un secondo punto P del piano, come nel disegno seguente[1].



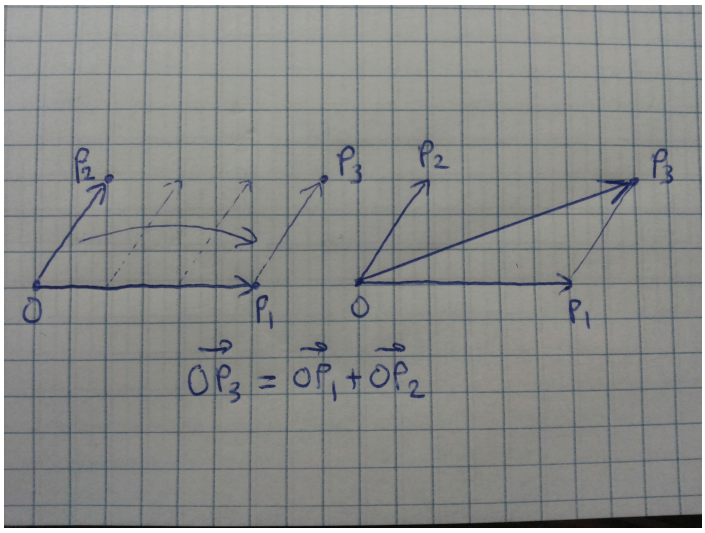
Analogamente, parliamo di *vettori geometrici applicati nello spazio* se il punto P (e quindi il segmento) è libero di variare in tutto lo spazio tridi-

[1] L'orientazione viene messa in evidenza con un simbolo di freccia

mensionale. In entrambi i casi il vettore sarà denotato $\vec{OP}$ (si noti che il punto finale P può anche essere uguale a O, ovvero il vettore può essere "schiacciato" sul punto O).
I vettori orientati sono importanti in fisica, dove vengono usati per rappresentare forze applicate sul punto O: ad esempio, si può immaginare che in O si trovi un oggetto sul quale viene esercitata una forza che lo "trascina" nella direzione e nel verso dati dalla freccia, mentre l'intensità della forza esercitata è rappresentata dalla lunghezza del segmento.

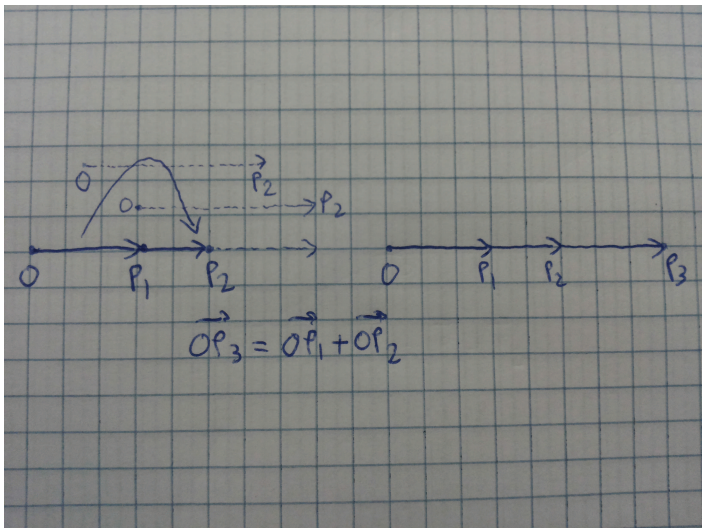
Con questa interpretazione, è naturale chiedersi cosa succede quando su O si esercitano contemporaneamente due forze rappresentate da due vettori geometrici $\vec{OP}_1$ e $\vec{OP}_2$: in tal caso, si verifica sperimentalmente che la forza totale "percepita" da O è quella rappresentata dal terzo vettore $\vec{OP}_3$ ottenuto nel modo seguente: si trasla parallelamente uno dei due vettori, diciamo $\vec{OP}_2$, in modo da spostare il suo punto di applicazione da O nel punto finale P_1 dell'altro vettore e si individua così il punto P_3 (si noti che si otterrebbe lo stesso punto se traslassimo invece $\vec{OP}_1$ spostando il suo punto di applicazione in P_2).
Dal momento che $\vec{OP}_3$ rappresenta la forza totale esercitata su O quando si applicano contemporaneamente $\vec{OP}_1$ e $\vec{OP}_2$, è naturale pensare $\vec{OP}_3$ come la somma di $\vec{OP}_1$ e $\vec{OP}_2$: scriveremo cioè

$$\vec{OP}_3 = \vec{OP}_1 + \vec{OP}_2$$



definendo in tal modo un'operazione di somma sull'insieme dei vettori geometrici (del piano o dello spazio).

Per vettori che non hanno la stessa direzione, si osserva che OP_3 è la diagonale del parallelogramma che ha OP_1 e OP_2 come lati (si parla infatti anche di *regola del parallelogramma*). Il metodo descritto funziona comunque anche per sommare due vettori che hanno la stessa direzione:

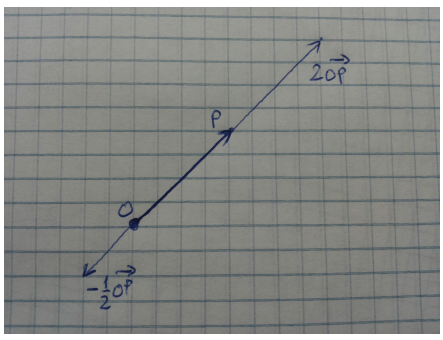


Un'altra operazione che si può introdurre nell'insieme dei vettori geometrici è il prodotto del vettore per un numero reale: nel contesto delle forze, l'idea è quella di rappresentare una variazione dell'intensità e eventualmente del verso della forza rappresentata dal vettore.
Più precisamente, dati un vettore geometrico $\vec{OP}$ e un numero reale $c \in \mathbb{R}$, definiamo $c\vec{OP}$ come il vettore che sta sulla stessa retta a cui appartiene $\vec{OP}$, ma avente:

(1) Stesso verso e lunghezza c volte la lunghezza di $\vec{OP}$, se c è positivo;

(2) Verso opposto e lunghezza $-c$ volte quella di $\vec{OP}$, se c è negativo;

(3) Lunghezza nulla se $c = 0$, cioè $0\vec{OP} = \vec{OO}$.



In questo contesto, i numeri reali si chiamano anche *scalari*.

Ora, come sappiamo e abbiamo visto in vari esempi nei capitoli precedenti, ogni volta che si introducono una o più operazioni su un insieme è bene conoscere le proprietà di cui godono tali operazioni: per quelle che abbiamo appena introdotto, si può verificare (con dimostrazioni di geometria euclidea, che omettiamo) che valgono le seguenti:

(1) La somma è *associativa*

$$(\vec{OP_1} + \vec{OP_2}) + \vec{OP_3} = \vec{OP_1} + (\vec{OP_2} + \vec{OP_3}) \tag{4.1}$$

(2) La somma è *commutativa*

$$\vec{OP_1} + \vec{OP_2} = \vec{OP_2} + \vec{OP_1} \tag{4.2}$$

(3) Il vettore $\vec{OO}$ funge da elemento neutro per la somma:

$$\vec{OP} + \vec{OO} = \vec{OO} + \vec{OP} = \vec{OP} \tag{4.3}$$

(4) Per ogni vettore $\vec{OP}$, il vettore $(-1)\vec{OP}$ (ovvero il vettore che si ottiene da $\vec{OP}$ semplicemente invertendo il verso, senza modificare direzione e lunghezza) è il suo inverso additivo o opposto rispetto alla somma:

$$\vec{OP} + (-1)\vec{OP} = (-1)\vec{OP} + \vec{OP} = \vec{OO} \tag{4.4}$$

(5) Dati due numeri reali c_1, c_2 e un vettore $\vec{OP}$, si ha

$$c_1(c_2\vec{OP}) = (c_1c_2)\vec{OP} \tag{4.5}$$

(una sorta di proprietà associativa del prodotto).

(6) Per ogni vettore $\vec{OP}$, si ha

$$1\vec{OP} = \vec{OP} \tag{4.6}$$

(ovvero il numero 1 funge da elemento neutro rispetto al prodotto per scalari).

(7) Dati due numeri reali c_1, c_2 e un vettore $\vec{OP}$, si ha

$$(c_1 + c_2)\vec{OP} = c_1\vec{OP} + c_2\vec{OP} \tag{4.7}$$

(8) Dati un numero reale c e due vettori $\vec{OP_1}$, $\vec{OP_2}$ si ha

$$c(\vec{OP_1} + \vec{OP_2}) = c\vec{OP_1} + c\vec{OP_2}. \tag{4.8}$$

(le ultime due ci dicono che vale la proprietà distributiva rispetto alla somma di numeri reali o rispetto alla somma di vettori).

Osservazione 4.1. Ispirati dall'esempio dei vettori geometrici, in matematica si definisce in generale *spazio vettoriale* un qualunque insieme i cui elementi possano essere sommati tra loro e moltiplicati per numeri reali (o più in generale per gli elementi di un campo), in modo che valgano proprietà analoghe alle (4.1)-(4.8), ma non approfondiamo in questo corso tale approccio astratto.

Come esempio di applicazione delle proprietà appena elencate, mostriamo che in una ugugaglianza tra vettori, esattamente come si fa in un'uguaglianza tra numeri, si possono"spostare i vettori" da un membro all'altro cambiandoli di segno:

$$\vec{OP_1} + \vec{OP_2} = \vec{OP_3} \ \rightarrow \ \vec{OP_1} = \vec{OP_3} - \vec{OP_2}$$

dove, come si fa anche per i numeri, stiamo scrivendo $\vec{OP_3} - \vec{OP_2}$ come forma semplificata di $\vec{OP_3} + (-1)\vec{OP_2}$.
Per vederlo, sommiamo a entrambi i membri di $\vec{OP_1} + \vec{OP_2} = \vec{OP_3}$ il vettore $(-1)\vec{OP_2}$:

$$(\vec{OP_1} + \vec{OP_2}) + (-1)\vec{OP_2} = \vec{OP_3} + (-1)\vec{OP_2}$$

Applichiamo la proprietà associativa (4.1) a primo membro:

$$\vec{OP_1} + (\vec{OP_2} + (-1)\vec{OP_2}) = \vec{OP_3} + (-1)\vec{OP_2}$$

Applichiamo la proprietà (4.4) che afferma che $(-1)\vec{OP_2}$ è l'opposto di $\vec{OP_2}$:

$$\vec{OP_1} + \vec{OO} = \vec{OP_3} + (-1)\vec{OP_2}$$

e infine applichiamo la (4.3) che ci dice che il vettore nullo funge da elemento neutro:

$$\vec{OP_1} = \vec{OP_3} + (-1)\vec{OP_2}$$

come volevamo.

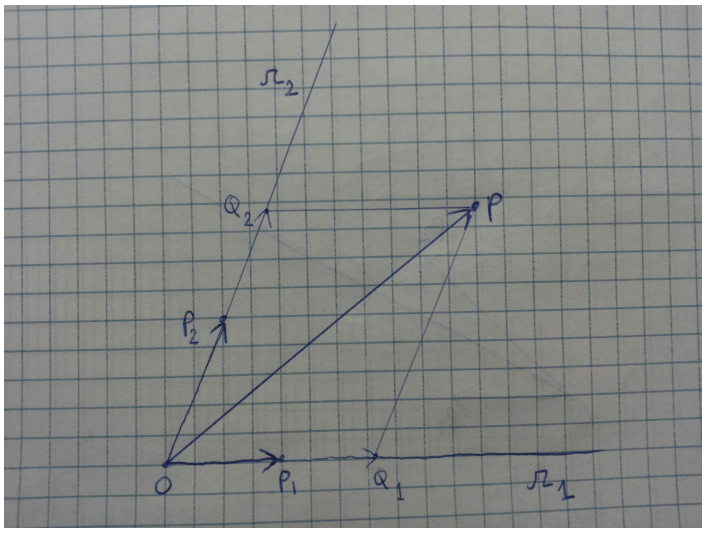
4.2 Coordinate

Consideriamo ora due vettori geometrici $\vec{OP_1}$ e $\vec{OP_2}$ nel piano, e supponiamo che $\vec{OP_1}$ e $\vec{OP_2}$ non abbiano la stessa direzione.
Affermiamo che ogni altro vettore può essere ottenuto sommando multipli opportuni di $\vec{OP_1}$ e $\vec{OP_2}$, ovvero

$$\vec{OP} = c_1\vec{OP_1} + c_2\vec{OP_2}$$

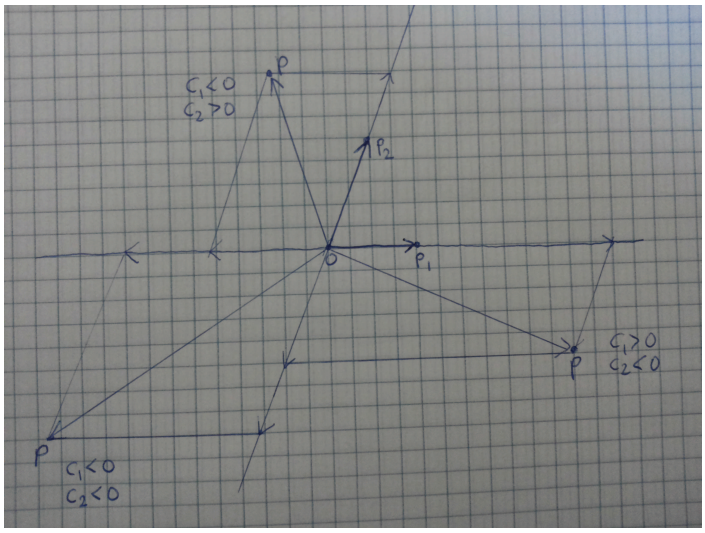
dove c_1, c_2 sono opportuni numeri reali.

Infatti, questo può essere facilmente visto graficamente: come nel disegno seguente, prolunghiamo i vettori $\vec{OP_1}$ e $\vec{OP_2}$ disegnando le due rette r_1 e r_2; proiettiamo quindi il punto P su r_1 seguendo la direzione parallela a $\vec{OP_2}$, e chiamiamo il punto proiettato Q_1; analogamente, proiettiamo il punto P su r_2 seguendo la direzione parallela a $\vec{OP_1}$, e chiamiamo il punto proiettato Q_2.



Avendo fatto le due proiezioni parallelamente a $\vec{OP_1}$ e $\vec{OP_2}$, risulta determinato un parallelogramma che ha $\vec{OQ_1}$ e $\vec{OQ_2}$ come lati e $\vec{OP}$ come diagonale, quindi per definizione di somma tra vettori geometrici si ha $\vec{OP} = \vec{OQ_1} + \vec{OQ_2}$.
Ma dal momento che $\vec{OQ_1}$ si trova sulla stessa retta di $\vec{OP_1}$, per come abbiamo definito il prodotto dei vettori per i numeri reali, esisterà un numero reale c_1 tale che $\vec{OQ_1} = c_1\vec{OP_1}$ (dove c_1 dipende semplicemente dal rapporto tra la lunghezza di $\vec{OQ_1}$ e quella di $\vec{OP_1}$) e analogamente esisterà un numero reale c_2 tale che $\vec{OQ_2} = c_2\vec{OP_2}$ (dove c_2 dipende dal rapporto tra la lunghezza di $\vec{OQ_2}$ e quella di $\vec{OP_2}$).
Abbiamo quindi concluso, come volevamo, che $\vec{OP} = c_1\vec{OP_1} + c_2\vec{OP_2}$.

Si noti che, nella situazione considerata nel disegno, $c_1, c_2 > 0$ in quanto $\vec{OQ_1}$ e $\vec{OQ_2}$ hanno lo stesso verso di $\vec{OP_1}$ e $\vec{OP_2}$ rispettivamente. In generale, la stessa costruzione può essere effettuata per qualunque vettore $\vec{OP}$ del piano e i coefficienti c_1 e c_2 potranno anche essere negativi[2] a seconda del quadrante nel quale si trova $\vec{OP}$, ovvero a seconda che la proiezione di P sulle rette r_1, r_2 cada dalla stessa parte o dalla parte opposta dei punti P_1 e P_2.



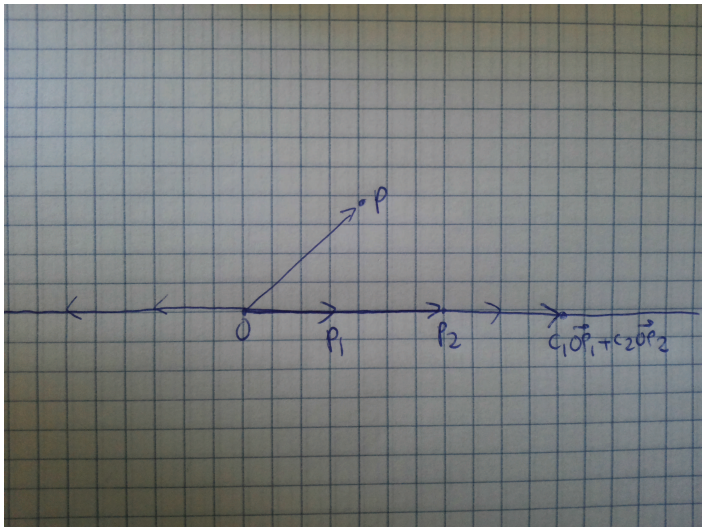
In ogni caso si avrà sempre $\vec{OP} = c_1\vec{OP_1} + c_2\vec{OP_2}$.

Diamo allora la seguente, importante

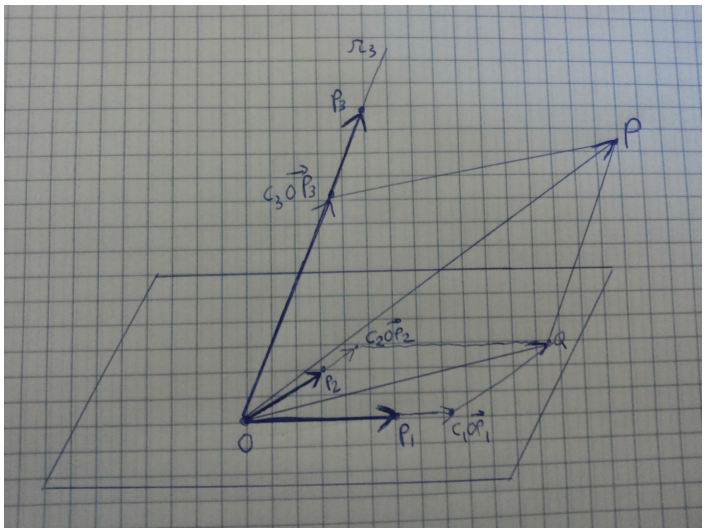
Definizione 4.2. Una coppia $\vec{OP_1}$ e $\vec{OP_2}$ di vettori non allineati nel piano si dice *base*. La coppia (c_1, c_2) di numeri reali tale che $\vec{OP} = c_1\vec{OP_1} + c_2\vec{OP_2}$ si dice la *coppia delle coordinate* del vettore $\vec{OP}$ rispetto a tale base (sottointendendo la base fissata, scriveremo anche $\vec{OP} \equiv (c_1, c_2)$).

Osservazione 4.3. Si noti che se prendiamo due vettori $\vec{OP_1}$ e $\vec{OP_2}$ *che stiano su una stessa retta* r, è facile vedere che non è più vero che ogni vettore si può scrivere come loro combinazione.
Infatti, qualunque multiplo $c_1\vec{OP_1}$ di $\vec{OP_1}$ sta ancora sulla retta r, analogamente qualunque multiplo $c_2\vec{OP_2}$ di $\vec{OP_2}$ sta su r, e quindi starà su r anche la somma $c_1\vec{OP_1} + c_2\vec{OP_2}$, e non riusciremo mai a ottenere come combinazione di $\vec{OP_1}$ e $\vec{OP_2}$ i vettori $\vec{OP}$ che stanno fuori dalla retta.

[2]Può essere anche $c_1 = 0$ o $c_2 = 0$: nel primo caso, si ha $\vec{OP} = c_2\vec{OP_2}$, nel secondo $\vec{OP} = c_1\vec{OP_1}$, cioè $\vec{OP}$ non sta all'interno di uno dei quadranti in cui le rette r_1, r_2 dividono il piano, ma sta sulla retta r_2 (se $\vec{OP} = c_2\vec{OP_2}$) o sulla retta r_1 (se $\vec{OP} = c_1\vec{OP_1}$).



Un risultato analogo a quello appena visto per i vettori nel piano può essere ottenuto anche nel caso dei vettori geometrici nello spazio tridimensionale. In questo caso non dobbiamo però partire da una coppia di vettori non allineati ma da una terna di vettori $\vec{OP}_1$, $\vec{OP}_2$ e $\vec{OP}_3$ *che non stiano tutti e tre sullo stesso piano*: allora, è facile vedere graficamente, utilizzando proiezioni come abbiamo fatto nel caso di due vettori nel piano, che ogni vettore $\vec{OP}$ dello spazio può essere scritto come combinazione $c_1\vec{OP}_1 + c_2\vec{OP}_2 + c_3\vec{OP}_3$.



Come rappresentato nel disegno, si proietta il punto P sul piano su cui stanno $\vec{OP}_1$ e $\vec{OP}_2$ seguendo la direzione di $\vec{OP}_3$ e si individua così un punto Q; proiettando poi P sulla retta r_3 parallelamente al vettore $\vec{OQ}$, risulta individuato un parallelogramma, che ci dice che $\vec{OP}$ si scrive come somma

$\vec{OP} = \vec{OQ} + c_3\vec{OP_3}$ di $\vec{OQ}$ e di un opportuno multiplo $c_3\vec{OP_3}$ di $\vec{OP_3}$. A questo punto si osserva che $\vec{OQ}$, stando sul piano di $\vec{OP_1}$ e $\vec{OP_2}$ si scriverà come loro combinazione lineare $\vec{OQ} = c_1\vec{OP_1} + c_2\vec{OP_2}$, e sostituendo nella $\vec{OP} = \vec{OQ} + c_3\vec{OP_3}$ si conclude che $\vec{OQ} = c_1\vec{OP_1} + c_2\vec{OP_2} + c_3\vec{OP_3}$.
In modo analogo a quanto già fatto per vettori geometrici del piano, possiamo allora dare la seguente

Definizione 4.4. Una terna $\vec{OP_1}$, $\vec{OP_2}$, $\vec{OP_3}$ di vettori non complanari nello spazio si dice *base*. La terna (c_1, c_2, c_3) di numeri reali tale che $\vec{OP} = c_1\vec{OP_1} + c_2\vec{OP_2} + c_3\vec{OP_3}$ si dice la *terna delle coordinate* del vettore $\vec{OP}$ rispetto a tale base (sottointendendo la base fissata, scriveremo anche $\vec{OP} \equiv (c_1, c_2, c_3)$).

L'importanza delle coordinate consiste nel fatto che esse, permettendoci di rappresentare i vettori mediante coppie o terne di numeri, ci permettono di tradurre in calcoli numerici i calcoli tra vettori: questa è innanzitutto un'importante semplificazione per noi, in quanto è più semplice lavorare con le coordinate che con costruzioni o dimostrazioni di geometria euclidea che sarebbero altrimenti necessarie per lavorare con i vettori, che sono oggetti geometrici; inoltre, tale traduzione è indispensabile se si vogliono far trattare tali problemi a un computer.
Per dare un'idea di queste affermazioni, mostriamo il seguente risultato:

Proposizione 4.5. Si fissi una base B nell'insieme dei vettori del piano. Allora

(1) Se $\vec{OP}$ e $\vec{OP'}$ hanno coordinate rispettivamente (x_1, x_2) e (x'_1, x'_2) rispetto a B, le coordinate di $\vec{OP} + \vec{OP'}$ rispetto a B sono date dalla coppia $(x_1 + x'_1, x_2 + x'_2)$ ottenuta sommando componente per componente le coppie delle coordinate dei due vettori.

(2) Se $\vec{OP}$ ha coordinate (x_1, x_2) rispetto a B e $c \in \mathbb{R}$ è un numero reale, allora le coordinate di $c\vec{OP}$ sono date dalla coppia (cx_1, cx_2) ottenuta moltiplicando per c le coordinate di $\vec{OP}$.

Proof. Siano $\vec{OP_1}$ e $\vec{OP_2}$ i vettori che costituiscono la base B fissata. Il fatto che $\vec{OP}$ abbia coordinate (x_1, x_2) rispetto a B significa per definizione che $\vec{OP} = x_1\vec{OP_1} + x_2\vec{OP_2}$, e analogamente il fatto che $\vec{OP'}$ abbia coordinate (x'_1, x'_2) rispetto a B significa che $\vec{OP'} = x'_1\vec{OP_1} + x'_2\vec{OP_2}$. Ma allora

$$\vec{OP} + \vec{OP'} = (x_1\vec{OP_1} + x_2\vec{OP_2}) + (x'_1\vec{OP_1} + x'_2\vec{OP_2}) =$$

(riordiniamo gli addendi e raccogliamoli diversamente sfruttando le proprietà associativa e commutativa della somma tra vettori)

$$= (x_1\vec{OP_1} + x_1'\vec{OP_1}) + (x_2\vec{OP_2} + x_2'\vec{OP_2}) =$$

(sfruttiamo la proprietà (4.7) sia nella prima parentesi che nella seconda)

$$= (x_1 + x_1')\vec{OP_1} + (x_2 + x_2')\vec{OP_2}$$

Ma questo, per definizione di coordinate, significa proprio che le coordinate di $\vec{OP} + \vec{OP'}$ sono date dalla coppia $(x_1 + x_1', x_2 + x_2')$, come affermato nella (1).

Per dimostrare la (2), partiamo sempre dal fatto che dire che $\vec{OP}$ abbia coordinate (x_1, x_2) rispetto a B significa per definizione che $\vec{OP} = x_1\vec{OP_1} + x_2\vec{OP_2}$. Allora

$$c\vec{OP} = c(x_1\vec{OP_1} + x_2\vec{OP_2}) =$$

(applichiamo la proprietà (4.8))

$$= c(x_1\vec{OP_1}) + c(x_2\vec{OP_2}) =$$

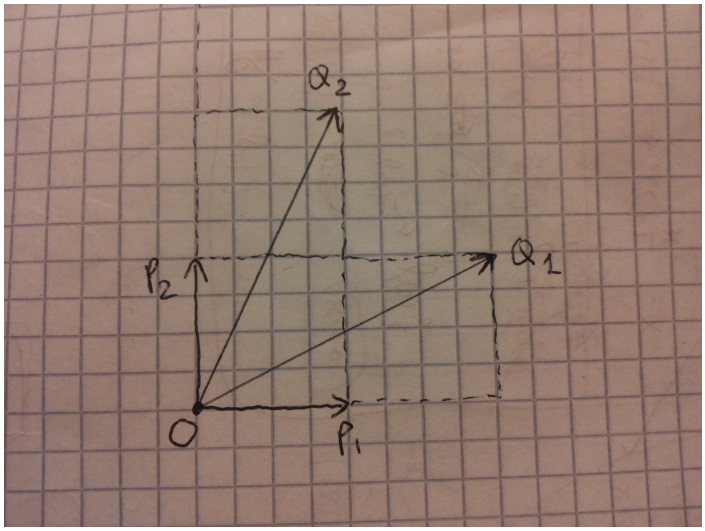
(applicando la (4.5) a entrambi gli addendi)

$$= (cx_1)\vec{OP_1} + (cx_2)\vec{OP_2}$$

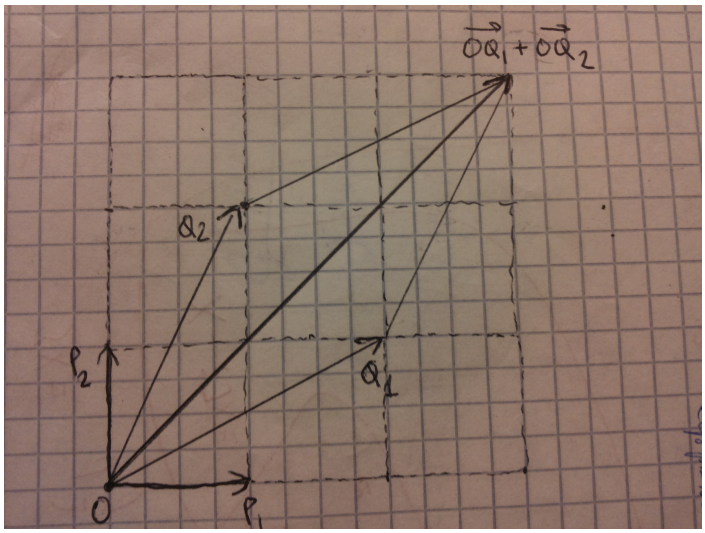
Ma questo, per definizione di coordinate, ci dice proprio che le coordinate di $c\vec{OP}$ sono date dalla coppia (cx_1, cx_2), come affermato nella (2).

□

Esempio 4.6. Per un esempio di quanto appena dimostrato, si considerino come nel disegno seguente la base $B = \{\vec{OP_1}, \vec{OP_2}\}$ e i due vettori $\vec{OQ_1}$ e $\vec{OQ_2}$



Come si vede graficamente, si ha $O\vec{Q}_1 = 2O\vec{P}_1 + O\vec{P}_2$ e $O\vec{Q}_2 = O\vec{P}_1 + 2O\vec{P}_2$, ovvero le coordinate di $O\vec{Q}_1$ rispetto alla base B sono date dalla coppia $(2, 1)$, mentre le coordinate di $O\vec{Q}_2$ rispetto alla base B sono date dalla coppia $(1, 2)$. Allora, in base alla (1) della Proposizione 4.5, la somma $O\vec{Q}_1 + O\vec{Q}_2$ ha coordinate (sempre rispetto alla base B) date da $(2 + 1, 1 + 2) = (3, 3)$, ovvero si ha $O\vec{Q}_1 + O\vec{Q}_2 = 3O\vec{P}_1 + 3O\vec{P}_2$.
In effetti, questo può essere verificato graficamente costruendo con la regola del parallelogramma la somma $O\vec{Q}_1 + O\vec{Q}_2$, come nel disegno seguente



La cosa notevole è che siamo stati in grado di dire chi era il vettore $O\vec{Q}_1 + O\vec{Q}_2$ (in coordinate) con un semplicissimo conto aritmetico, anche prima di disegnarlo con la costruzione geometrica del parallelogramma.

Osservazione 4.7. Affermazioni del tutto analoghe a quelle della Proposizione 4.5 valgono anche nel caso dei vettori nello spazio tridimensionale, e la dimostrazione è perfettamente analoga a quella appena vista per il piano. Più precisamente, si ha che fissata una base B nell'insieme dei vettori dello spazio tridimensionale, allora

(1) Se $\vec{OP}$ e $\vec{OP'}$ hanno coordinate rispettivamente (x_1, x_2, x_3) e (x'_1, x'_2, x'_3) rispetto a B, le coordinate di $\vec{OP} + \vec{OP'}$ rispetto a B sono date dalla terna $(x_1 + x'_1, x_2 + x'_2, x_3 + x'_3)$ ottenuta sommando componente per componente le terne delle coordinate dei due vettori.

(2) Se $\vec{OP}$ ha coordinate (x_1, x_2, x_3) rispetto a B e $c \in \mathbb{R}$ è un numero reale, allora le coordinate di $c\vec{OP}$ sono date dalla terna (cx_1, cx_2, cx_3) ottenuta moltiplicando per c le coordinate di $\vec{OP}$.

Osservazione 4.8. Il fatto che, fissata una base, ogni vettore del piano (risp. dello spazio tridimensionale) sia determinato in modo univoco da una coppia (risp. una terna) di numeri reali, ci dice che l'insieme dei vettori del piano (risp. dello spazio tridimensionale) si può identificare con l'insieme $\mathbb{R}^2$ (risp. $\mathbb{R}^3$). La Proposizione 4.5 ci dice inoltre che lavorare con l'insieme dei vettori geometrici dotato della somma e del prodotto per scalari definito all'inizio del capitolo è la stessa cosa che lavorare con $\mathbb{R}^2$ o $\mathbb{R}^3$ dotati della somma e del prodotto per numeri reali definiti nel modo seguente:

$$(x_1, x_2) + (x'_1, x'_2) := (x_1 + x'_1, x_2 + x'_2), \quad c(x_1, x_2) := (cx_1, cx_2)$$

$$(x_1, x_2, x_3) + (x'_1, x'_2, x'_3) := (x_1 + x'_1, x_2 + x'_2, x_3 + x'_3), \quad c(x_1, x_2, x_3) := (cx_1, cx_2, cx_3).$$

In generale, in uno spazio n-dimensionale avremmo dovuto usare lo spazio $\mathbb{R}^n$ dotato della somma e del prodotto definiti da

$$(x_1, x_2, \ldots, x_n) + (x'_1, x'_2, \ldots, x'_n) := (x_1 + x'_1, x_2 + x'_2, \ldots, x_n + x'_n)$$

$$c(x_1, x_2, \ldots, x_n) := (cx_1, cx_2, \ldots, cx_n).$$

Notiamo che lo spazio $\mathbb{R}^n$, oltre ad essere la rappresentazione in coordinate di un ipotetico spazio n-dimensionale (che per alcune teorie fisiche è una possibilità concreta) può rappresentare un qualunque insieme o sistema in cui servano più di 3 parametri indipendenti, non necessariamente che rappresentino solo la posizione spaziale, per descriverne gli elementi: ad esempio, $\mathbb{R}^4$ potrebbe rappresentare l'insieme dei punti dello spazio tridimensionale con un'informazione aggiuntiva (la quarta componente) che può ad esempio essere la temperatura in quel punto (o la frequenza di un colore da associare a quel punto, se stiamo traducendo numericamente un disegno).