GLI INSIEMI NUMERICI

Si presentano qui alcune nozioni sugli insiemi numerici, con l'obiettivo di ricordarne le proprietà elementari e qualche risultato classico.

Prerequisiti[1]: insiemi, funzioni, relazioni d'equivalenza e d'ordine, operazioni e loro proprietà, strutture algebriche, calcolo combinatorio.

Contenuto:

§ 1 I numeri naturali: preistoria; gli assiomi di Peano, operazioni, potenze, divisori e multipli, ordinamenti, il principio del minimo.

§ 2 I numeri interi relativi come numeri naturali col segno: ordinamento, valore assoluto e segno, operazioni; l'anello dei numeri interi.

§ 3 Divisibilità in $\mathbf{N}$ ed in $\mathbf{Z}$: divisione col resto, massimo comune divisore e minimo comune multiplo, algoritmo euclideo, identità di Bézout, numeri primi e teorema fondamentale dell'aritmetica; equazioni diofantee; congruenze mod m, gli anelli quoziente $\mathbf{Z}_n$ ed i loro elementi invertibili, la funzione di Eulero.

§ 4 I numeri razionali: dal monoide $(\mathbf{N}, +)$ al gruppo $(\mathbf{Z}, +)$ e dal monoide $\left(\mathbf{N}^+, \cdot\right)$ al gruppo $\left(\mathbf{Q}^+, \cdot\right)$. Il campo razionale.

§ 5 I numeri reali: campi ordinati, completezza e continuità, isomorfismo, cenni alle costruzioni di $\mathbf{R}$; numeri decimali periodici e non periodici, qualche idea sulle operazioni con numeri decimali illimitati.

§ 6 I numeri complessi: costruzione formale; il piano di Argand-Gauss; i numeri complessi come vettori, la forma trigonometrica, la formula di De Moivre; Il campo complesso come insieme di opportune matrici reali quadrate d'ordine 2 e come anello quoziente $\mathbf{R}[x]/\left(x^2+1\right)$. Non ordinamento del campo complesso.

[1] Per ciascuno dei prerequisiti si veda il documento o la scheda con lo stesso nome.

§ 1 – I NUMERI NATURALI

Si possono introdurre i *numeri naturali* come file finite di *tacche*:

1 = I 2 = II 3 = III e così via.

Lo *zero* è l'assenza di tacche. E' un metodo che dal punto di vista teorico permette di capire facilmente le operazioni ed il confronto.

- L'*ordinamento* è evidente: si sovrappongono le due file di tacche e quella che "sporge" è maggiore dell'altra.
- *Addizionare* non è altro che giustapporre:

  III+IIII = IIIIIII

  e così ogni numero è somma di tanti 1 quante sono le sue tacche.
- *Sottrarre* è eliminare dal minuendo tante tacche quante sono espresse dal sottraendo, purché sia minore o uguale al minuendo:

  IIIII - II = III
- *Moltiplicare* è addizionare successivamente lo stesso numero di tacche:

  III × II = II+II+II = IIIIII
- *Dividere* è sottrarre successivamente il divisore dal dividendo, finché possibile: il *quoziente* è il numero delle sottrazioni, il *resto* è quel che rimane alla fine.

Le proprietà sono quasi immediate. In particolare, persino uno scoglio concettuale come la divisione per zero è facile: sottrarre zero tacche da un numero dato non lo cambia mai, si può proseguire all'infinito e non si ha un quoziente ed un resto, perciò non ha senso dividere per zero.

Questo metodo si pensa sia stato il primo ad essere utilizzato nella storia della rappresentazione dei numeri: infatti il più antico ritrovamento consiste in un osso di lupo, risalente a 30.000 anni fa circa, con incise una successione di tacche a distanza all'incirca costante l'una dall'altra e con una tacca più lunga in corrispondenza di cinque tacche corte.

Tuttavia, questo approccio non è soddisfacente ai tempi nostri: i numeri come tacche diventano presto ingestibili e le esigenze di calcolo e di

introduzione di nuovi insiemi di numeri (per misurare e non solo per contare) richiedono una razionalizzazione dei numeri naturali.

In questa sezione si richiama la definizione secondo Peano dell'insieme $\mathbf{N} = \{0, 1, 2, ...\}$ dei numeri naturali; successivamente si introducono le operazioni di addizione e moltiplicazione di $\mathbf{N}$ e le relative relazioni d'ordine e ne sono descritte le proprietà principali.

Per la comprensione del testo sono richieste alcune nozioni elementari su insiemi, relazioni d'equivalenza e d'ordine, funzioni e operazioni.

Assiomi di Peano. L'insieme $\mathbf{N}$ dei numeri naturali può essere definito mediante gli assiomi di Peano, che, con il linguaggio degli insiemi, tradurremo nel modo seguente:

I. $\mathbf{N}$ contiene un elemento, indicato con 0.

II. E' definita una funzione iniettiva $\sigma : \mathbf{N} \xrightarrow{1\text{–}1} \mathbf{N}$, la cui immagine è $\mathbf{N} \setminus \{0\}$

III. Per ogni $M \subseteq \mathbf{N}$, se $0 \in M$ e se per ogni $n \in M$ anche $\sigma(n) \in M$, allora $M = \mathbf{N}$.

In altre parole, la III postula che ogni sottoinsieme M contenente lo zero e che sia *chiuso* rispetto a σ coincide con $\mathbf{N}$. Per ogni $n \in \mathbf{N}$, l'elemento $\sigma(n)$ è detto *successivo* di n. Dalla proprietà II segue che $\mathbf{N}$ è infinito. Si può provare inoltre che ogni insieme con queste proprietà è equipotente ad $\mathbf{N}$ e viene detto *numerabile*.

La proprietà III si chiama *principio d'induzione* e si usa in definizioni e dimostrazioni che coinvolgano una variabile $n \in \mathbf{N}$.

Le *dimostrazioni per induzione* seguono lo schema seguente: si debba provare un'affermazione P(n) che abbia senso per ogni numero naturale.

a) Si dimostra innanzitutto che è vera P(0).
b) Si dimostra che l'essere vera P(n) (*ipotesi induttiva*) implica che è vera $P(\sigma(n))$.

In tal modo l'insieme M dei numeri n per i quali P(n) è vera contiene 0 e per ogni $n \in M$ contiene anche $\sigma(n)$. Dunque, per il principio d'induzione, $M = \mathbf{N}$.

Analogamente, la proprietà III serve per definire nozioni, secondo lo schema seguente (*definizioni ricorsive*): si debba definire una nozione, che denoteremo con D(n), e che abbia senso per ogni numero naturale.

a) Si definisce esplicitamente D(0).
b) Supposta definita D(n), si definisce mediante essa D(σ(n)).

In tal modo l'insieme M dei numeri n per i quali D(n) è definita contiene 0 e per ogni n∈M contiene anche σ(n). Dunque, per il principio d'induzione, M = **N**.

A volte si parte da un numero n_0 anziché da 0. In tal caso, l'affermazione P(n) sarà provata solo per ogni $n \geq n_0$. Analogamente per le definizioni D(n).

Osservazione. In alcuni casi, per dimostrare un'affermazione P(n) si segue uno schema un po' diverso, detto *II principio d'induzione*:

a) si dimostra P(0)
b) supposto vero P(k) per ogni $k \leq n$, si dimostra P(σ(n)).

Esempi di dimostrazioni per induzione e di definizioni ricorsive si troveranno nel seguito. Incominciamo con il definire le operazioni.

Addizione. Su **N** si può definire ricorsivamente la *somma* di un numero m con un numero n qualsiasi, nel modo seguente:

$$\begin{cases} m+0=m \\ m+\sigma(n)=\sigma(m+n) \end{cases}$$

In tal modo, per la proprietà III, per ogni m∈**N** la *somma* m+n è definita per ogni n∈**N**. Posto 1 = σ(0), si ottiene subito, per ogni m∈**N**:

$$\sigma(m) = \sigma(m+0) = m+\sigma(0) = m+1.$$

Chiamiamo *addizione* l'operazione $+ : \mathbf{N}^2 \to \mathbf{N}$, $+ : (m,n) \mapsto m+n$, che associa a una coppia ordinata (m, n) di numeri naturali la loro somma.

PROPOSIZIONE 1.1. - L'addizione possiede le proprietà seguenti:
a) *associativa*: per ogni a, b, c∈**N** risulta: (a+b)+c = a+(b+c);

b) *elemento neutro*: per ogni a∈**N** si ha a+0 = 0+a = a;

c) *commutativa*: per ogni a, b∈**N** risulta a+b = b+a.

Dimostrazione. a) L'uguaglianza è vera per c = 0, risultando (a+b)+0 = a+b = a+(b+0).

Supponendola provata per c = n (ipotesi induttiva), dimostriamo che è vera per c = σ(n) nel modo seguente:

$$(a+b)+c = (a+b)+\sigma(n) =$$

(per la definizione di +) $= \sigma((a+b)+n) =$

(per l'ipotesi induttiva) $= \sigma(a+(b+n)) =$

(per la definizione di +) $= a+\sigma(b+n) =$

(ancora per la definizione di +) $= a+(b+\sigma(n)) = a+(b+c)$,

come si voleva.

b) Per definizione di + si ha a+0 = a. L'uguaglianza 0+a = a è vera ovviamente per a = 0. Supponendola provata per a = n, se a = σ(n) si ha:

$$0+a = 0+\sigma(n) = \sigma(0+n) = \sigma(n) = a.$$

c) La dimostrazione della proprietà commutativa è più complessa, perché occorre procedere per induzione rispetto ad entrambi gli addendi. Per b) la proprietà è vera se a = 0. Sia vera per a = n e dimostriamo che è vera per a = σ(n). Per questo procediamo per induzione rispetto a b.

E' vera per definizione di + se b = 0. Sia vera per b = m. Per b = σ(m) si ha allora:

$$a+b = \sigma(n)+\sigma(m) = \sigma(\sigma(n)+m) =$$

(per l'ipotesi induttiva su b) $= \sigma(m+\sigma(n)) = \sigma(\sigma(m+n)) =$

(per l'ipotesi induttiva su a) $= \sigma(\sigma(n+m)) = \sigma(n+\sigma(m)) =$

(ancora per l'ipotesi induttiva su a) $= \sigma(\sigma(m)+n) = \sigma(m)+\sigma(n) = b+a$,

così come si voleva.

Col linguaggio dell'algebra possiamo concludere che la terna (**N**, +, 0) risulta un *monoide* commutativo. Esso possiede inoltre le seguenti proprietà:

PROPOSIZIONE 1.2. - Ulteriori proprietà dell'addizione.

a) Per ogni a, b∈**N**, se a+b = 0 allora a = b = 0.

b) *Legge di cancellazione*: per ogni a, b, c∈**N**, se a+b = a+c allora b = c.

c) Per ogni a, b∈**N**, una e, se a ≠ b, una sola delle due equazioni: $\begin{cases} a + x = b \\ b + y = a \end{cases}$, nelle incognite x, y∈**N**, ha soluzione, ed in tal caso ne ha una sola.

Dimostrazione. Sia a ≠ 0. Per induzione su b proviamo che a+b ≠ 0. Innanzi tutto, a+0 = a ≠ 0. Sia a+b ≠ 0. Allora a+σ(b) = σ(a+b) ≠ 0 perché 0∉σ(**N**).

Pertanto, può essere a+b = 0 solo se a = 0, ma allora b = 0+b = 0 implica b = 0.

b) Sia a+b = a+c. Se a = 0 si ha b = c. Sia vero per a = n. Allora, per a = σ(n) si ha: a+b = σ(n)+b = σ(n+b), e analogamente a+c = σ(n+c). Perciò, da a+b = a+c segue σ(n+b) = σ(n+c), da cui, per la iniettività di σ, si ha n+b = n+c. Per l'ipotesi induttiva segue allora b = c.

c) Per induzione rispetto a b proviamo che una delle due equazioni ha soluzione. Se b = 0 allora si ha y = a. Sia vero per b = n. Sia ora b = n+1. Se si aveva a+x = n, allora a+(x+1) = n+1 = b. Invece nel caso n+y = a, se y = 0 si ha anche a+0 = a, per cui siamo nel caso precedente; se y ≠ 0, allora y appartiene all'immagine di σ e quindi esiste z tale che z+1 = σ(z) = y.

Allora b+z = (n+1)+z = n+(1+z) = n+y = a.

Se risulta contemporaneamente a+x = b e b+y = a, per la proprietà associativa si ha: b+0 = b = a+x = (b+y)+x = b+(y+z), quindi per la legge di cancellazione si ha y+z = 0, ma per a) si ha y = z = 0 e quindi b = a. La soluzione è unica per la legge di cancellazione.

Sottrazione. Se risulta a+d = b, si pone b-a = d e d si chiama *differenza* di b ed a. In particolare si ha a-a = 0.

Moltiplicazione. Si definisce ricorsivamente l'operazione di *moltiplicazione* · definendo dapprima il *prodotto* di un m per un n qualsiasi, nel modo seguente (ricordando che σ(n) = n+1):

$$\text{per ogni m, n}\in\mathbf{N},\ \begin{cases} m \cdot 0 = 0 \\ m \cdot (n+1) = m \cdot n + m \end{cases}.$$

Di conseguenza, per esempio, m·1 = m·(0+1) = m·0+m = m, ecc. Solitamente il *prodotto* di m per n si denota con mn, anziché con m·n. La moltiplicazione è l'operazione che ad ogni coppia (m,n) associa il prodotto m·n

PROPOSIZIONE 1.3. - Proprietà della moltiplicazione.

1) *Elemento assorbente*: per ogni a∈**N**, 0·a = a·0 = 0
2) *Elemento neutro*: per ogni a∈**N** si ha a·1 = 1·a = a.
3) *Distributiva* rispetto al +: per ogni a, b, c∈**N** risulta $\begin{cases}(a+b)c = ac + bc \\ a(b+c) = ab + ac\end{cases}$
4) *Associativa*: per ogni a, b, c∈**N** risulta (ab)c = a(bc)
5) *Commutativa*: per ogni a, b∈**N** risulta ab = ba.

Dimostrazione. 1) Basta provare che si ha 0·a = 0. E' vera per a = 0. Sia vera per a, allora $0 \cdot \sigma(a) = 0 \cdot a + 0 = 0 + 0 = 0$, quindi è vero anche per $\sigma(a)$.

2) $a \cdot 1 = a \cdot \sigma(0) = a \cdot 0 + a = 0 + a = a$. Invece, $1 \cdot 0 = 0$ e, supposto 1·a = a, allora si ha $1 \cdot \sigma(a) = 1 \cdot a + 1 = a + 1 = \sigma(a)$ e anche la 2) è dimostrata.

3) Vediamo la prima uguaglianza, ossia la *distributività a sinistra*. Se c = 0 entrambi i membri sono nulli, quindi per c = 0 l'uguaglianza è vera. Sia c un numero per il quale l'uguaglianza è vera. Allora, usando la definizione di prodotto, l'ipotesi su c e le proprietà della somma, si ha:

$$(a+b)\cdot\sigma(c) = (a+b)\cdot c + (a+b) = a\cdot c + b\cdot c + a + b =$$
$$= (a\cdot c + a) + (b\cdot c + b) = a\cdot\sigma(c) + b\cdot\sigma(c)$$

Vediamo la *distributività a destra*. Se a = 0 è vera. Sia vera per un a∈**N**; allora, usando questa informazione, la proprietà di 1 e la prima uguaglianza, si ha:

$$\sigma(a)\cdot(b+c) = (a+1)\cdot(b+c) = a\cdot(b+c) + (b+c) = ab + ac + b + c =$$
$$= (a\cdot b + 1\cdot b) + (a\cdot c + 1\cdot c) = (a+1)\cdot b + (a+1)\cdot c = \sigma(a)\cdot b + \sigma(a)\cdot c$$

4) Per induzione su c: se c = 0 è vero. Sia c un numero per il quale si ha (ab)c = a(bc). Allora, per la proprietà distributiva e l'ipotesi induttiva si ha:

$$(ab)\cdot\sigma(c) = (ab)\cdot c + ab = a\cdot(bc) + ab = a\cdot(bc + b) = a\cdot(b\cdot\sigma(c))$$

Quindi è vero anche per $\sigma(c)$.

5) E' vero se b = 0. Sia b tale che ab = ba. Allora:

$$a\cdot\sigma(b) = a\cdot b + a = b\cdot a + 1\cdot a = (b+1)\cdot a = \sigma(b)\cdot a$$

Pertanto anche la terna ($\mathbf{N}$, $\cdot$, 1) risulta un monoide commutativo. Esso possiede inoltre le seguenti proprietà:

PROPOSIZIONE 1.4. - Ulteriori proprietà della moltiplicazione.

a) L'unico elemento dotato di *inverso* è 1, cioè per ogni a, b$\in\mathbf{N}$, se ab = 1 allora a = b = 1.

b) *Legge di annullamento del prodotto*: per ogni a, b$\in\mathbf{N}$ si ha ab = 0 se e solo se a = 0 oppure b = 0.

Si osservi che nel monoide ($\mathbf{N}$, $\cdot$, 1) la *legge di cancellazione* non vale, a causa della presenza dello 0; infatti per ogni a, b si ha a·0 = b·0 = 0. Pertanto da a·0 = b·0 non segue necessariamente a = b.

Consideriamo però il sottoinsieme $\mathbf{N}^+ = \mathbf{N}\setminus\{0\}$: la legge di annullamento del prodotto ha come conseguenza che se a, b$\in\mathbf{N}^+$ anche ab$\in\mathbf{N}^+$. Poiché inoltre 1$\in\mathbf{N}^+$, possiamo considerare il *sottomonoide* ($\mathbf{N}^+$, $\cdot$, 1). In esso valgono le seguenti proprietà:

PROPOSIZIONE 1.5. - Proprietà del monoide ($\mathbf{N}^+$, $\cdot$, 1).

a) *Legge di cancellazione*: per ogni a, b, c$\in\mathbf{N}^+$, se ab = ac allora b = c.

b) Per ogni a, b$\in\mathbf{N}^+$ al massimo una delle due equazioni $\begin{cases} a\cdot x = b \\ b\cdot y = a \end{cases}$, nelle incognite x ed y$\in\mathbf{N}^+$, ha soluzione. Tale soluzione, se esiste, è unica (per la legge di cancellazione).

A differenza dell'analoga proprietà dell'addizione, la proprietà 1.5.b della moltiplicazione non contiene l'affermazione dell'esistenza, ma solo dell'unicità dell'eventuale soluzione.

Divisione. Dati a, b$\in\mathbf{N}^+$, se risulta aq = b allora q si dice *quoziente* di "b diviso a" e si pone b:a = q. In particolare, b:b = 1.

Osservazione. Poiché per ogni a $\neq$ 0 risulta a·0 = 0, si può definire il quoziente di

0 diviso a, ponendo 0:a = 0. Non ha senso invece la scrittura 0:0, in quanto per ogni q∈**N** si ha 0·q = 0.

L'ordine naturale. L'ordine naturale di **N** si può definire a partire dall'addizione, ponendo per ogni a, b∈**N**,

$$a \le b \text{ se esiste } d \in \mathbf{N} \text{ tale che } a+d = b.$$

PROPOSIZIONE 1.6. - Proprietà della relazione ≤:

a) *Proprietà riflessiva*: per ogni a∈**N** si ha a ≤ a.

b) *Proprietà antisimmetrica*: per ogni a,b∈**N**, se a ≤ b e b ≤ a allora a = b.

c) *Proprietà transitiva:* per ogni a, b, c∈**N**, se a ≤ b e b ≤ c allora a ≤ c.

d) *Dicotomia*: per ogni a, b∈**N** si ha ≤ b oppure b ≤ a.

Dimostrazione. a) Per ogni a∈**N** si ha: a+0 = a, quindi a ≤ a.

b) Se a+m = b e b+n = a allora a+(m+n) = a, ed essendo a = a+0, per la legge di cancellazione si ha m+n = 0, da cui segue m = n = 0 e a = b.

c) Da a+m = b, b+n = c segue a+(m+n) = c.

d) Basta applicare la proprietà 1.2.c.

Le prime tre proprietà hanno come conseguenza che (**N**, ≤) è un *insieme ordinato* e la quarta che l'ordine è *totale*. Inoltre, poiché per ogni n∈**N** si ha 0+n = n allora 0 ≤ n. Dunque 0 è il *minimo*. Non c'è invece *massimo*, poiché per ogni n∈**N** si ha n < n+1. Inoltre:

PROPOSIZIONE 1.7. - Relazioni tra operazioni ed ordine.

a) Per ogni a, b, c∈**N**, si ha a ≤ b se e solo se a+c ≤ b+c.

b) Per ogni n∈**N**, se n ≤ x ≤ n+1 allora x = n oppure x = n+1.

Dimostrazione. a) Da a+m = b segue (a+c)+m = (b+c) e viceversa.

b) Se n < x allora x = n+m, con 1 ≤ m, quindi n+1 ≤ n+m = x ≤ n+1 ⇒ x = n+1.

Sia H un sottoinsieme di **N**. Un elemento x∈**N** si dice *minorante* di H se per ogni h∈H si ha x ≤ h. Si dice *minorante stretto* se per ogni h∈H si ha x < h.

PROPOSIZIONE 1.8 (principio del minimo). - Ogni sottoinsieme non vuoto H di **N** possiede il minimo.

Dimostrazione. Se $0\in H$ allora 0 è il suo minimo. Sia $0\notin H$ e sia M(H) l'insieme dei minoranti stretti di H. Innanzitutto, $H\cap M(H)=\varnothing$. Inoltre, $0\in M(H)$. Se per ogni $x\in M(H)$ si avesse anche $x+1\in M(H)$ allora, per il principio d'induzione, $M(H)=\mathbf{N}$ ed $H=H\cap\mathbf{N}=H\cap M(H)=\varnothing$, assurdo. Dunque, esiste $x_0\in M(H)$ tale che $x_0+1\in H$. Ne segue che x_0+1 è il minimo cercato: infatti ogni altro $h\in H$ è maggiore di x_0, quindi per 1.7.b) è anche $h\geq x_0+1$.

L'ordine dalla divisibilità. Eseguiamo una 'traduzione' in notazione moltiplicativa delle nozioni precedenti, per introdurre un ordine in $\mathbf{N}^+$. Definiamo la relazione $|$ (*divide*) in $\mathbf{N}^+$ ponendo:

per ogni $a, b\in\mathbf{N}^+$, $a \mid b$ se esiste $q\in\mathbf{N}^+$ tale che $aq = b$.

Sostituendo $\leq$ con $|$ e 0 con 1 nella proposizione 1.6, mediante le proprietà della moltiplicazione si provano subito le seguenti proprietà:

PROPOSIZIONE 1.9. - Proprietà della relazione $|$:

a) *Proprietà riflessiva*: per ogni $a\in\mathbf{N}^+$ si ha $a \mid a$.

b) *Proprietà antisimmetrica*: per ogni $a,b\in\mathbf{N}^+$, se $a \mid b$ e $b \mid a$ allora $a = b$.

c) *Proprietà transitiva:* per ogni $a, b, c\in\mathbf{N}^+$, se $a \mid b$ e $b \mid c$ allora $a \mid c$.

Non vale invece la dicotomia: per esempio 2 non divide 3 e 3 non divide 2. Queste proprietà ci dicono che $(\mathbf{N}^+, |)$ è un insieme *parzialmente ordinato*. Inoltre, poiché per ogni $n\in\mathbf{N}^+$ si ha $1\cdot n = n$ allora $1 \mid n$. Dunque 1 è il minimo. Non c'è invece massimo, poiché per ogni $n\in\mathbf{N}^+$ si ha per esempio $n \mid 2n$. L'ordinamento $|$ di $\mathbf{N}^+$ è legato all'ordinamento $\leq$ dalla relazione seguente:

PROPOSIZIONE 1.10. - Per ogni $a, b\in\mathbf{N}^+$, se $a \mid b$ allora $a \leq b$. Inversamente, se $a < b$ allora b non divide a.

Dimostrazione. Sia $b = aq$ e procediamo per induzione rispetto a q. Se $b = a\cdot 1$ allora $a = b$, quindi $a \leq b$. Supponiamo vero il teorema per $q = n$ (ipotesi

induttiva) e proviamolo per q = n+1. Sia b = a(n+1) = an+a: per ipotesi induttiva e per la proposizione 1.7 si ha:

$$a \le an = an + 0 \le an+a = b,$$

da cui segue $a \le b$. Inversamente, se $a < b$ e se fosse $b \mid a$ allora $b \le a$, assurdo.

Osservazione. Volendo estendere l'ordinamento $\mid$ a tutto $\mathbf{N}$, si deve porre necessariamente $n \mid 0$ per ogni $n \in \mathbf{N}$, in particolare, $0 \mid 0$. Infatti per ogni $n \in \mathbf{N}$ esiste almeno un elemento $q \in \mathbf{N}$, tale che $nq = 0$: ovviamente, è $q = 0$ (e non è richiesta l'unicità di q). Pertanto $(\mathbf{N}, \mid)$ oltre al minimo, uguale ad 1, possiede anche il massimo, lo zero.

Potenze. Nel monoide $(\mathbf{N}^+, \cdot, 1)$ per ogni $a \in \mathbf{N}^+$ e per ogni $n \in \mathbf{N}$ si definisce ricorsivamente la *potenza* a^n nel modo seguente:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}.$$

In particolare si ha $a^1 = a$. Per le potenze valgono le seguenti proprietà, che si dimostrano per induzione rispetto ad n:

PROPOSIZIONE 1.11. - Per ogni $a, b \in \mathbf{N}^*$ e per ogni $m, n \in \mathbf{N}$ si ha:

a) $a^m \cdot a^n = a^{m+n}$

b) $(a^m)^n = a^{mn}$

c) $(ab)^n = a^n b^n$

Osservazione. Mentre le prime proprietà dipendono solo dalla definizione di potenza e dalla proprietà associativa della moltiplicazione, la terza dipende in modo essenziale dalla proprietà commutativa: $(ab)^2 = abab = aabb = a^2b^2$.

Quanto sopra detto per le potenze si può ripetere per il monoide $(\mathbf{N}, +\ 0)$. Osserviamo che, in notazione additiva, la potenza di base a ed esponente n si scrive *na* anziché a^n, e si ha:

$$\begin{cases} 0a = 0 \\ (n+1)a = na + a \end{cases}.$$

Il numero *na* si chiama *multiplo naturale* di a.

PROPOSIZIONE 1.12. - Altre proprietà di multipli e potenze.

a) Per ogni n, h, k∈**N**, n ≠ 0, si ha h < k se e solo se hn < kn. In particolare, l'unico multiplo di n che sia minore di n è lo zero.

b) Per ogni n, h, k∈$\mathbf{N}^+$, n ≠ 1, si ha h < k se e solo se $n^h < n^k$ (o equivalentemente se e solo se n^h divide "propriamente" n^k). In particolare, l'unica potenza di n che sia minore di n (cioè divisore proprio di n) è 1.

Nota. Per le definizioni ricorsive, a volte accade che esista un $h > 0$ tale che D(n+h) dipenda da D(n), ..., D(n+h-1). In tal caso occorre definire esplicitamente D(0), D(1), ..., D(h-1) (*condizioni iniziali*). Un esempio è dato dai *numeri di Fibonacci*:

$$\begin{cases} a_0 = 1 \\ a_1 = 1 \\ a_{n+2} = a_n + a_{n+1} \end{cases} \Rightarrow \begin{array}{c|cccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline a_n & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 21 \end{array} \ldots$$

Circa i concetti legati alla divisibilità, ossia massimo comune divisore e minimo comune multiplo, numeri primi, scomposizione in fattori primi, se ne riparlerà diffusamente nella terza sezione e nel capitolo sugli anelli, ma, naturalmente, si tratta di concetti noti fin dalla scuola media inferiore.

§ 2 – I NUMERI INTERI RELATIVI

L'impossibilità di eseguire sempre la sottrazione nell'insieme **N** dei numeri naturali ha portato alla costruzione dei numeri *interi relativi*, o semplicemente dei *numeri interi*.

Elementarmente, si possono definire coppie formate da un *segno,* + oppure -, e da un numero naturale: +7, -12, -35, +35.

Le coppie +0 e -0 si considerano coincidenti e individuano un intero che si denota solo con 0.

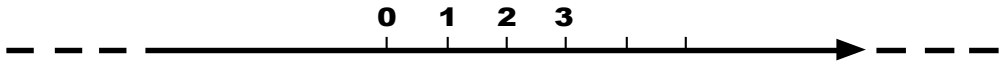
L'insieme ottenuto si denota con:

$$\mathbf{Z} = \{0, +1, -1, +2, -2, +3, -3, \ldots\}.$$

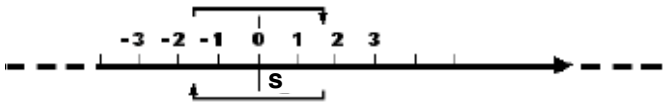
Per comodità, il segno + di solito non si scrive. Chiamiamo *negativi* i numeri col segno - e *positivi* quelli col +.

"Identifichiamo" gli interi positivi con i naturali.

Sia data una retta r, su cui siano fissati un punto O, una unità di misura u e un orientamento. Possiamo distribuire i numeri naturali 0, 1, 2, ... sulla semiretta positiva, facendoli corrispondere ai multipli del segmento unità di misura.



L'effetto del segno – è quello di scambiare, con una rotazione s di 180° intorno ad O, la semiretta positiva con quella negativa.



Perciò, per ogni $x \in \mathbf{Z}$, $-(-x) = x$.

L'ordinamento. Definiamo l'ordine $\leq$ in **Z**:

- Lo zero è maggiore di ogni numero negativo e minore di ogni positivo.
- Sui positivi l'ordine coincide con quello naturale di **N**:

$$+3 < +5 \text{ perché } 3 < 5$$

- Sui negativi l'ordine è opposto, perché il segno – opera una simmetria rispetto all'origine: $-5 < -3$ perché $3 < 5$

L'ordine $\leq$ è totale ed è una *estensione* di quello di **N**: sui numeri positivi coincide infatti con quello di **N**.

Il successivo. La funzione σ ("successivo di") si prolunga da **N** a **Z** ponendo $\forall m, n \in \mathbf{N}$:

$$\sigma(-m) = -n \Leftrightarrow \sigma(n) = m$$

Si ha così: $\sigma : \mathbf{Z} \xrightarrow[\text{su}]{1\text{–}1} \mathbf{Z}$. In particolare, si ha $0 = \sigma(-1)$. Inoltre, esiste σ^{-1}.

Valore assoluto e segno. Ad ogni intero x associamo un intero $|x| \geq 0$, ed un altro intero $\text{sign}(x) \in \{-1, 1\}$, definiti da:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}, \quad \text{sign}(x) = \begin{cases} 1 & \text{se } x > 0 \\ -1 & \text{se } x < 0 \end{cases}.$$

$|x|$ è il valore assoluto di x; sign(x) è il segno di x ed è definito solo per $x \neq 0$.

Operazioni. Le operazioni in **Z** sono costruite in modo che sui numeri positivi coincidano con quelle di N, ed inoltre siano compatibili con il segno.

In particolare, $\forall a \in \mathbf{Z}, \forall n \in \mathbf{N}$ si può definire l'addizione a+n nel modo seguente:

$$\begin{cases} a + 0 = a \\ a + \sigma(n) = \sigma(a + n) \end{cases} \quad \begin{cases} a + (-1) = \sigma^{-1}(a) \\ a + (-\sigma(n)) = \sigma^{-1}(a + (-n)) \end{cases}$$

Geometricamente, σ è una traslazione di una unità nel verso positivo, mentre σ^{-1} è una traslazione di una unità nel verso negativo. Allora:

$$a + n = \sigma^{n}(a), \; a + (-n) = \sigma^{-n}(a)$$

Poi si definisce la moltiplicazione:

$$\begin{cases} a \cdot 0 = 0 \\ a \cdot \sigma(n) = a \cdot n + a \end{cases} \qquad \begin{cases} a \cdot (-1) = -a \\ a \cdot (-n) = (-a) \cdot n \end{cases}$$

Le due operazioni + e · hanno le proprietà associativa e commutativa; hanno gli elementi neutri (0 per l'addizione ed 1 per la moltiplicazione), ed ogni elemento x ha l'opposto –x, tale che $x + (-x) = 0$. Inoltre, come in **N**, la moltiplicazione è *distributiva* rispetto all'addizione:

$$\forall a, b, c \in \mathbf{Z}: (a+b)\cdot c = a\cdot c + b\cdot c$$

Ricordiamo la *regola dei segni* per la moltiplicazione:

·	+	–
+	+	–
–	–	+

Ricordiamo infine che vale la *legge d'annullamento del prodotto*:

$$\forall a, b \in \mathbf{Z},\ a\cdot b = 0 \Rightarrow a = 0 \text{ oppure } b = 0$$

Elementi invertibili. I soli elementi con inverso rispetto alla moltiplicazione sono 1 e -1, ossia:

$$\mathbf{Z}^* = \{x \in \mathbf{Z} \mid \exists y \in \mathbf{Z},\ x \cdot y = 1\} = \{1, -1\}$$

La divisibilità. Si può procedere come in **N**, ma c'è la complicazione dei segni: ogni numero $a \in \mathbf{Z}$ è infatti divisore anche del suo opposto: $a = (-1)\cdot(-a)$.
Per esempio, un numero p è primo se ha per divisori solo 1, -1, p, -p.

Conviene pensare ogni numero negativo come ottenuto moltiplicando il suo opposto (che è positivo) per -1. In tal modo, i conti si svolgono sempre con numeri positivi.

Esempio di scomposizione in fattori primi:

$$-18 = (-1)\cdot 18 = (-1)\cdot 2\cdot 3^2.$$

Valgono allora in **Z** il teorema fondamentale dell'aritmetica, l'algoritmo euclideo e l'esistenza ed unicità del MCD e del mcm, di cui parleremo nella prossima sezione.

Osservazione. Una diversa costruzione di **Z** sarà accennata nella quarta sezione.

§ 3 – L'ALGORITMO EUCLIDEO E APPLICAZIONI

PROPOSIZIONE 3.1. Divisione col resto in N. Dati due numeri naturali a, b, con $b \neq 0$, esistono due numeri naturali q, r, univocamente determinati, tali che $\begin{cases} a = b \cdot q + r \\ 0 \leq r < b \end{cases}$.

Dimostrazione: se $a < b$ allora $q = 0$ ed $r = a$. Se $a \geq b$ sia $M = \{a - b \cdot k \mid k \in \mathbf{N}\}$: non è vuoto perché $a \in M$, perciò ha minimo $r \geq 0$. Allora esiste q tale che $r = a - b \cdot q$, e si ha $r < b$, altrimenti $s = r-b = a-(q+1)b \in M$ e $s < r$, assurdo. Se poi si ha anche $a = b \cdot q' + r'$, con per esempio $r' < r$, allora:

$$b \cdot q + r = b \cdot q' + r' \Rightarrow r - r' = b \cdot (q' - q), \text{ con } q'-q \geq 1.$$

Ma si ha contemporaneamente $r - r' < r < b \leq b \cdot (q' - q)$, assurdo. Dunque si ha l'unicità di q ed r.

PROPOSIZIONE 3.2. Divisione col resto in Z. Dati due numeri interi a, b, con $b \neq 0$, esistono due numeri interi q, r tali che $\begin{cases} a = b \cdot q + r \\ |r| < |b| \end{cases}$. L'unicità si ha se si impone $r \geq 0$.

Dimostrazione. Identifichiamo i numeri interi non negativi con i numeri naturali. Se esiste un intero q tale che $a = b \cdot q$ siamo a posto: $r = 0$.

Sia a non multiplo di b. Allora esistono q', r' non negativi tali che $\begin{cases} |a| = |b| \cdot q' + r' \\ 0 \leq r' < |b| \end{cases}$.

Si tratta ora di esaminare le quattro possibilità:

a	b	quoziente q	resto r
> 0	> 0	q'	r'
> 0	< 0	-q'	r'
< 0	> 0	-(q'+1)	b-r'
< 0	< 0	q'+1	|b|-r'

Nei quattro casi si trovano sempre un quoziente ed un resto. L'unicità si dimostra come nel caso dei numeri naturali.

LEMMA 3.3. Siano a, b due numeri interi non nulli. Siano q, r il quoziente ed il resto della divisione di a per b. Allora ogni divisore comune di a e b è divisore comune anche di b ed r, e viceversa.

Dimostrazione: Si ha $a = b \cdot q + r$, allora $r = a - b \cdot q$. Sia c un divisore comune di a e b. Allora esistono h, k interi tali che $\begin{cases} a = c \cdot h \\ b = c \cdot k \end{cases}$. Ne segue $r = c \cdot (h - k \cdot q)$, quindi c divide anche r. Inversamente, sia s un divisore comune di b ed r: esistono m, n interi tali che $\begin{cases} b = s \cdot m \\ r = s \cdot n \end{cases}$, quindi $a = s \cdot (m + n \cdot q)$ ed s divide anche a.

Il *massimo comune divisore* MCD(a,b) di due interi a e b è un divisore comune di a e b, multiplo di ogni altro divisore comune. Non è unico, a causa del segno, ma possiamo convenire sia positivo. Circa la sua esistenza, vediamo il prossimo risultato:

PROPOSIZIONE 3.4. - Algoritmo euclideo delle divisioni successive. Siano a, b due numeri interi non nulli. Allora:

i) esiste $d = MCD(a, b)$

ii) esistono u, v interi tali che $a \cdot u + b \cdot v = d$. (*Identità di Bézout*)

Dimostrazione. Sappiamo che ogni divisore comune di a e b è divisore comune anche di ±a e di ±b. Perciò supponiamo a e b positivi.

Supponiamo $b \le a$ e siano q, r il quoziente ed il resto della divisione di a per b. Se $r = 0$ allora $d = b$. Sia $r \neq 0$. Per il lemma, i divisori comuni di b ed r sono divisori comuni anche di a e b e viceversa. Dividiamo allora b per r: esistono q_1, r_1 interi tali che $\begin{cases} b = r \cdot q_1 + r_1 \\ 0 \le r_1 < r \end{cases}$. Se $r_1 = 0$ allora $d = r = MCD(b,r) = MCD(a,b)$.

Se $r_1 \neq 0$ dividiamo r per r_1 ottenendo: $\begin{cases} r = r_1 \cdot q_2 + r_2 \\ 0 \le r_2 < r_1 \end{cases}$.

Procediamo allo stesso modo dividendo ogni volta il divisore per il resto ed otteniamo una successione di quozienti e di resti: $\begin{cases} r_n = r_{n+1} \cdot q_{n+2} + r_{n+2} \\ 0 \le r_{n+2} < r_{n+1} \end{cases}$.

Ad ogni nuova divisione il resto è minore del resto della divisione precedente, sicché dopo un numero finito m di passi arriviamo finalmente ad un resto r_{m+1} nullo. Allora:

$$r_m = \mathrm{MCD}(r_{m-1}, r_m) = \mathrm{MCD}(r_{m-2}, r_{m-1}) = \ldots = \mathrm{MCD}(a, b)$$

e quindi $d = r_m$.

Poniamo ora $r_{-1} = b,\ r_0 = r$. Poiché $b = a \cdot 0 + b \cdot 1,\ r = a \cdot 1 + b \cdot (-q) r$, allora poniamo $\begin{cases} u_{-1} = 0 \\ v_{-1} = 1 \end{cases}, \begin{cases} u_0 = 1 \\ v_0 = -q \end{cases}$. Per induzione su $n \ge 0$ supponiamo esistano quattro interi $u_{n-1}, v_{n-1}, u_n, v_n$ tali che $\begin{cases} r_{n-1} = a \cdot u_{n-1} + b \cdot v_{n-1} \\ r_n = a \cdot u_n + b \cdot v_n \end{cases}$. Allora da $r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$ segue:

$$r_{n+1} = r_{n-1} - r_n \cdot q_{n+1} = a \cdot u_{n-1} + b \cdot v_{n-1} - (a \cdot u_n + b \cdot v_n) \cdot q_{n+1} =$$

$$= a \cdot (u_{n-1} - q_{n+1} \cdot u_n) + b \cdot (v_{n-1} - q_{n+1} \cdot v_n)$$

Perciò: $\begin{cases} u_{n+1} = u_{n-1} - q_{n+1} \cdot u_n \\ v_{n+1} = v_{n-1} - q_{n+1} \cdot v_n \end{cases}$. In particolare, ciò vale anche per $d = r_m$, quindi

$$\begin{cases} u = u_{m-2} - q_m \cdot u_{m-1} \\ v = v_{m-2} - q_m \cdot v_{m-1} \end{cases}.$$

Si può costruire uno schema che riproduca direttamente il procedimento induttivo visto sopra, fornendo sia d sia i coefficienti u e v.

a	b	$r_0 = r$	r_1	r_2	...
1	0	$u_0 = 1 - 0 \cdot q_0$	$u_1 = 0 - u_0 \cdot q_1$	$u_2 = u_0 - u_1 \cdot q_2$	
0	1	$v_0 = 0 - 1 \cdot q_0$	$v_1 = 1 - v_0 \cdot q_1$	$v_2 = v_0 - v_1 \cdot q_2$	
	$q_0 = q$	q_1	q_2	q_3	

Esempio con a = 120 e b = 85:

120	85	35	15	5	0
1	0	1	-2	5	-17
0	1	-1	3	-7	24
	1	2	2	3	

Si osservi che si ha:

35=120·1+85·(-1)	15=120·(-2)+83·3	5=120·5+85·(-7)	0=120·(-17)+83·24

L'ultimo resto non nullo è 5, quindi 5 = MCD(120, 85) = 120·5 + 85·(-7)

COROLLARIO 3.5. a)Due numeri interi a, b non nulli sono coprimi (ossia MCD(a,b) = 1) se e solo se esistono u, v interi tali che $a \cdot u + b \cdot v = 1$.

b) Sia d = MCD(a,b). Posto a = d·a', b = d·b' allora MCD(a',b') = 1.

Dimostrazione. a) I due numeri a, b sono coprimi se MCD(a, b) = 1, quindi per l'algoritmo euclideo esistono u, v interi tali che $a \cdot u + b \cdot v = 1$. Inversamente, posto d = MCD(a, b), se esistono u, v interi tali che $a \cdot u + b \cdot v = 1$, allora necessariamente d divide 1, quindi è uguale ad 1, per cui a e b sono coprimi.

b) Siano u, v tali che $a \cdot u + b \cdot v = d$. Dividiamo per d ambo i membri ed otteniamo $a' \cdot u + b' \cdot v = 1$, quindi per a) si ha MCD(a',b') = 1.

COROLLARIO 3.6. Lemma di Euclide. Dati tre numeri interi a, b, c, se a divide bc e MCD(a,b) = 1, allora a divide c.

Dimostrazione. Sia bc = aq. Per il corollario 3.5. esistono u, v interi tali che $1 = a \cdot u + b \cdot v$. Allora, moltiplicando ambo i membri per c, otteniamo:

$$c = a \cdot (cu) + (bc) \cdot v = a \cdot (cu + qv)$$

In **N** un numero > 1 si dice *primo* (o *indecomponibile*) se ha come divisori solo se stesso e 1. Un numero primo si caratterizza nel modo seguente:

PROPOSIZIONE 3.7. Un numero naturale p > 1 è primo se e solo se ogni volta che divide un prodotto m·n di interi, divide almeno uno dei fattori.

Dimostrazione. Sia p primo e supponiamo divida m·n. Essendo p primo, allora MCD(p,m) = p oppure = 1. Nel primo caso, p divide m e siamo a posto; nel secondo, per il lemma di Euclide p divide n.

Viceversa, supponiamo che p sia tale che se divide un prodotto m·n allora divide uno dei fattori. Se p non è primo, allora ha dei divisori propri r, s, tali che $p = r \cdot s$. Ne segue $r \cdot s = p \cdot 1$, ossia p divide il prodotto $r \cdot s$; allora divide uno dei

fattori, per esempio r, ma in tal caso p ed r sono uguali, mentre s = 1, contro l'ipotesi che siano divisori propri. Dunque, p è primo.

TEOREMA 3.8. Teorema fondamentale dell'aritmetica. Ogni numero naturale maggiore di 1 è primo oppure è prodotto di fattori primi, e due di queste scomposizioni differiscono solo per l'ordine dei fattori.

Dimostrazione. Sia M l'insieme dei numeri naturali > 1 per i quali il teorema è falso. Per assurdo sia $M \neq \emptyset$. Allora possiede il minimo, che denotiamo con m. Si ha quindi m > 1, e per m il teorema non vale. In particolare, se m non è primo, è prodotto di due divisori propri r, s, ossia $m = r \cdot s,\ 1 < r, s < m$. Allora per r ed s il teorema vale, quindi sono primi o prodotto di primi ed anche m è prodotto dei primi di r per i primi di s. Dunque, m è primo o prodotto di primi. Poiché per m il teorema non è vero, deve cadere l'unicità, ossia m si scrive in due modi diversi come prodotto di primi: $m = p_1 \cdot p_2 \cdot \cdots \cdot p_r = q_1 \cdot q_2 \cdot \cdots \cdot q_s$, r, s ≥ 1. Poiché p_1 è primo, per la proposizione 3.7 dividendo il prodotto $q_1 \cdot q_2 \cdot \cdots \cdot q_s$, deve dividere almeno uno dei suoi fattori, per esempio q_1. Ma q_1 è a sua volta primo, quindi $p_1 = q_1$. Possiamo semplificare per p_1 ed ottenere il numero $m' = p_2 \cdot \cdots \cdot p_r = q_2 \cdot \cdots \cdot q_s$, minore di m. Se m' = 1 allora $m = p_1$, unica possibilità, ma non può essere, perché per m il teorema è falso, ed allora $1 < m' < m$, quindi per m' il teorema è vero e si ha l'unicità della scomposizione, ossia le due fattorizzazioni di m' hanno r-1 = s-1 fattori e, a meno di riordini, si ha $p_i = q_i,\ 2 \leq i \leq r$. Ne segue l'unicità anche per m, assurdo. Pertanto, questo m non esiste, $M = \emptyset$, ed il teorema è vero per ogni n > 1.

TEOREMA 3.9. (Euclide) In **N** esistono infiniti numeri primi.

Dimostrazione. Per assurdo ce ne siano un numero finito r e siano $p_1, p_2, \ldots, p_r$. Sia $n = p_1 \cdot p_2 \cdot \cdots \cdot p_r + 1$: essendo maggiore di tutti i primi, n non è primo, però è prodotto di primi. Sia p uno di essi. Se p fosse uno dei $p_1, p_2, \ldots, p_r$, allora p dividerebbe anche $1 = n - p_1 \cdot p_2 \cdot \cdots \cdot p_r$, quindi p non è uno di quegli r, che però per ipotesi erano tutti i numeri primi, assurdo.

In **Z** ogni numero diverso da 0 e da ±1 ha come divisori almeno se stesso, l'opposto e ±1, ossia ha almeno 4 divisori. È primo se ha solo questi quattro. Il

teorema fondamentale vale anche in **Z**, a patto di considerare l'unicità a meno non solo dell'ordine dei fattori, ma anche dei segni di alcuni di essi. Su questo argomento torneremo nel capitolo degli anelli, nel quale ricorderemo anche le tecniche per il calcolo di MCD ed mcm di due numeri o due polinomi.

EQUAZIONI DIOFANTEE. Le equazioni algebriche in una o più incognite a coefficienti interi e di cui si cercano le soluzioni intere si *chiamano equazioni diofantee*. Se sono di I grado sono dette *lineari*. Hanno molte applicazioni nei settori più svariati non solo della Matematica pura, ma anche nella tecnologia e curiosamente anche nell'Enigmistica. Persino il Cinema se ne è occupato, a proposito del cosiddetto "ultimo teorema di Fermàt", dimostrato però da Wales qualche anno fa, sull'impossibilità di soluzioni intere dell'equazione diofantea $x^n + y^n = z^n$ non appena sia $n > 2$.

Tralasciando quelle in una incognita, ci occupiamo delle equazioni diofantee lineari in due incognite: $ax + by = c$. Supporremo cioè nel seguito che a e b siano non nulli. Come sempre, occorre esaminare i tre aspetti del problema: esistenza di soluzioni, numero delle soluzioni, algoritmi risolutivi. Siano nel seguito: d = MCD(a, b), a = da', b = db'.

LEMMA 3.10. Esistenza. Esiste una soluzione dell'equazione diofantea $ax + by = c$ se e solo se d = MCD(a,b) divide c.

Dimostrazione. Siano x, y interi tali che ax+by = c. Allora:

$$c = ax + by = da'x + db'y = d(a'x + b'y)$$

quindi d divide c. D'altra parte, se d divide c, posto c = dc', per l'algoritmo euclideo esistono u, v interi tali che au + bv = d, quindi:

$$a(c'u) + b(c'v) = c'd = c$$

e una soluzione (x, y) = (c'u, c'v) esiste.

LEMMA 3.11. Numero soluzioni. Se esiste una soluzione dell'equazione diofantea $ax + by = c$ allora ce ne sono infinite

Dimostrazione. Sia (u, v) una soluzione dell'equazione $ax + by = c$. Consideriamo *l'equazione omogenea associata* ax+by = 0. Dividiamo per d ed otteniamo

$a'x + b'y = 0$, ossia a'x = -b'y. Poiché MCD(a', b') = 1, allora, per il lemma di Euclide, a' divide y, ossia esiste k intero tale che y = ka'. Ma allora x = -kb'. Inversamente, per ogni k intero, la coppia (-kb', ka') è soluzione dell'equazione omogenea associata.

Pertanto, per ogni k intero si ha

$$a(u-kb') + b(v+ka') = au + bv + a(-kb') + b(ka') = c+0 = c,$$

ossia la coppia $(u - k \cdot b', v + k \cdot a')$ è soluzione dell'equazione data per ogni k intero. Inversamente, per ogni altra soluzione (u', v') dell'equazione data, la differenza $(u' - u, v' - v)$ è soluzione dell'equazione omogenea associata. Allora esiste k intero tale che $\begin{cases} u' - u = -k \cdot b \\ v' - v = k \cdot a \end{cases}$, ossia $\begin{cases} u' = u - k \cdot b \\ v' = v + k \cdot a \end{cases}$.

Abbiamo così un insieme numerabile di soluzioni, una per ogni k intero.

ALGORITMI RISOLUTIVI. Un algoritmo per risolvere l'equazione diofantea lineare ax + by = c, in cui d = MCD(a, b) e c = dc', è già stato indicato:

- con l'algoritmo euclideo si determinano u, v tali che au + bv = d
- si trova la soluzione particolare $(x_0, y_0) = (u \cdot c', v \cdot c')$
- si aggiungono le soluzioni dell'equazione omogenea associata:

$$(x, y) = (x_0 - k \cdot b', y_0 + k \cdot a'),\ k \in \mathbf{Z}.$$

Tuttavia, la soluzione particolare potrebbe essere migliorata, nel senso che potrebbe essere utile "minimizzarla".

ESEMPIO 3.12. Vediamo l'equazione diofantea:

$$120x + 85y = 50$$

Si ha MCD(120, 85) = 5, che divide 50. Allora risolviamo dapprima l'equazione

$$120u + 85v = 5, \text{ (o anche } 24u + 17v = 1).$$

Le soluzioni le sappiamo: u = 5, v = -7. Poiché c' = 50/5 = 10, si ha così:

$$(x_0, y_0) = (u \cdot c', v \cdot c') = (50, -70)$$

Si ha poi a' = 120/5 = 24, b' = 85/5 = 17. Pertanto, la soluzione generale è:

$$(x, y) = (x_0 - k \cdot b', y_0 + k \cdot a') = (50 - 17k, -70 + 24k),\ k \in \mathbf{Z}.$$

Per migliorare la forma delle soluzioni, dividiamo 50 per 17, ottenendo quoziente 2 e resto 16, oppure quoziente 3 e resto -1.
Nel primo caso si ha 50 – 17k = 16 – 17k', dove k' = k-2, e si ha anche

$$-70+24k = -70+24(k'+2) = -22+24k'.$$

Perciò (x, y) = (16-17k', -22+24k'), k'∈**Z**.
Nel secondo caso, posto k" = k+3, si ha $\begin{cases} x = -1+17k'' \\ y = 2+24k'' \end{cases}$, k" ∈**Z**. Quest'ultima forma delle soluzioni è assai più semplice delle precedenti.

NOTA. Sia $(x,y) = (50-17k, -70+24k)$ la soluzione trovata con l'algoritmo. Facciamo variare per il momento k in **R** e cerchiamo la soluzione di norma minima. Minimizziamo cioè x^2+y^2 al variare di k. Ossia, minimizziamo la funzione $f(k) = 865k^2 - 5060k + 7400$. Annullando la derivata di f, (oppure, per chi non sa le derivate, prendendo l'ascissa k del vertice della parabola grafico di questa funzione), troviamo $k = \frac{506}{173} \approx 2,92$. Gli interi più prossimi sono $k = 2$ e $k = 3$, ma 3 è più vicino al valore trovato. Per questi due valori interi di k si trovano le due soluzioni particolari (16, -22) e (-1, 2) già note, e la seconda è migliore dell'altra.
Nel caso generale di ax + by = c si trova $k = \frac{-(a' \cdot y_0 - b' \cdot x_0)}{a'^2 + b'^2}$.

CONGRUENZE MODULO m. *L'aritmetica modulare* è in realtà un ambiente in cui ci troviamo ogni giorno, poiché la nostra vita è piena di fenomeni periodici discreti o discretizzati: i giorni della settimana, le ore del giorno, i mesi, le stagioni, i giornali quotidiani, gli orari per assumere antibiotici, ecc. La curiosità del matematico viene stimolata spesso proprio da fatti consueti come questi e portata a indagare più a fondo per trovare proprietà, estensioni, applicazioni forse impensate.

Sia m un numero intero. Per ogni x, y∈**Z** poniamo:

$x \equiv y \pmod m$ se x-y è multiplo di m

e diciamo che x è congruo ad y modulo m. Si ha subito che se $x \equiv y \pmod m$ allora si ha anche $x \equiv y \pmod{-m}$. Pertanto, possiamo supporre $m \geq 0$.

E' noto dal capitolo sulle nozioni di base che la congruenza modulo m è una relazione d'equivalenza nell'insieme **Z** degli interi relativi. Denotiamo con $[x]_n$ la classe di equivalenza di X e con $\mathbf{Z}_n$ l'insieme quoziente.

Se m = 0 la congruenza modulo m coincide con l'identità, poiché x-y è multiplo di 0 se e solo se x-y = 0. Pertanto, per ogni $x \in \mathbf{Z}$, $[x]_m = \{x\}$ e l'insieme quoziente $\mathbf{Z}_0$ coincide (sostanzialmente) con **Z**.

Se m = 1, essa coincide invece col prodotto cartesiano $\mathbf{Z} \times \mathbf{Z}$, poiché x-y è sempre multiplo di 1 e quindi tutte le coppie di interi sono in relazione mod 1. Pertanto, c'è un'unica classe d'equivalenza, e $\mathbf{Z}_1 = \{\mathbf{Z}\}$. Escludiamo nel seguito questi due casi banali.

Denotiamo con mod(x,m) il resto della divisione di x per m. Si ha:

a) Per ogni $x \in \mathbf{Z}$, si ha sempre $x \equiv \mathrm{mod}(x,m) \pmod m$.

b) Per ogni $x, y \in \mathbf{Z}$ si ha $x \equiv y \pmod m$ se e solo se $\mathrm{mod}(x,m) = \mathrm{mod}(y,m)$.

Pertanto, il numero delle classi di equivalenza di questa relazione eguaglia il numero di resti possibili, cioè n, e:

$$\mathbf{Z}_m = \{[r]_m \mid 0 \leq r < m\}$$

Osservazione. Questa relazione di congruenza modulo m si può definire anche nell'insieme N dei numeri naturali, ma non con la definizione iniziale, che non darebbe una relazione simmetrica (se x > y, x-y esiste in N, ma y-x no). O si mette la condizione che m divida la differenza max{x,y}-min{x,y}, oppure si usa la precedente proprietà b).

Ricordiamo ora che la congruenza mod m è *compatibile* con le operazioni dell'anello **Z**, nel senso che, se $a \equiv a' \pmod m$ e $b \equiv b' \pmod m$, allora:

$$a+a' \equiv b+b' \pmod m,\ a \cdot a' \equiv b \cdot b' \pmod m$$

Pertanto, possiamo definire fra le classi d'equivalenza le *operazioni quoziente*:

$$[x]_m + [y]_m = [x+y]_m,\ [x]_m \cdot [y]_m = [x \cdot y]_m,$$

ed ottenere così l'*anello quoziente*, nel quale lo zero è $[0]_m$, l'opposto di $[x]_m$ è $[-x]_m$ e l'unità è $[1]_m$. In relazione all'osservazione precedente, possiamo notare che la dimostrazione di queste proprietà è semplice in **Z**, ma molto più complicata in **N**.

Consideriamo ora *l'insieme delle unità* $\mathbf{Z}_m^*$, costituito dagli elementi dotati di inverso moltiplicativo.

LEMMA 3.13. Un elemento $[a]_m \in \mathbf{Z}_m$ è invertibile se e solo se MCD(a,m) = 1.

Dimostrazione. MCD(a,m) = 1 $\Leftrightarrow \exists u,v \in \mathbf{Z}$ tali che au+mv = 1. Dividiamo u per m, ottenendo u = mq+r, con 0 < r < m, quindi

$$1 = au+mv = ar+(aq+v)m \Rightarrow [1]_m = [a]_m\,[r]_m$$

ed allora $[a]_m$ è invertibile ed ha $[r]_m$ per inversa.

Inversamente, se $[a]_m$ ha per inverso $[r]_m$ si ha: 1 = mod(ar,m), ossia esiste q tale che ar+mq = 1 e ciò implica MCD(a,m) = 1.

Poniamo ora $\varphi(m) = |\{a \in \mathbf{Z} \mid 1 \le a \le m,\ MCD(m,a) = 1\}|$. Ossia, $\varphi(m)$ è il numero di interi tra 1 ed m, primi con m. La funzione $\varphi : \mathbf{Z}^+ \to \mathbf{Z}^+$ è detta *funzione di Eulero*.

Pertanto, $\mathbf{Z}_m^* = \left\{ [a]_m \in \mathbf{Z}_m \;\middle|\; MCD(a,m) = 1 \right\}$ ha $\varphi(m)$ elementi.

Osservazione. La funzione di Eulero si può calcolare anche con la formula seguente: se $m = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, dove $p_1, \ldots, p_k$ sono primi distinti, allora $\varphi(m) = m \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$. Infatti, si può dimostrare che per ogni a, b coprimi, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ e che per ogni numero primo p si ha $\varphi(p^n) = p^n - p^{n-1} = p^n \cdot \left(1 - \frac{1}{p}\right)$. Per esempio,

$$\varphi(117000) = \varphi(2^3 \cdot 3^2 \cdot 5^2 \cdot 13^1) = 117000 \cdot \left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{3}\right) \cdot \left(1-\frac{1}{5}\right) \cdot \left(1-\frac{1}{13}\right) = 28800$$

La descrizione di $\mathbf{Z}_n = \{[r]_m \mid 0 \le r < n\}$ non è maneggevole, a causa delle parentesi quadre che circondano i rappresentanti. Possiamo per semplicità identificare le classi con i rappresentanti *canonici* costituiti dai resti della divisione per n, e operare su di essi. Poniamo pertanto:

$$\mathbf{Z}_m = \{0, 1, \dots, m-1\}.$$

Si pone allora il problema di trovare come l'addizione e la moltiplicazione quoziente operino sui rappresentanti canonici. E' molto semplice:

il rappresentante di $[x]_m + [y]_m$ è $\quad \mathrm{mod}(x+y,n)$

il rappresentante di $[x]_m \cdot [y]_m$ è $\quad \mathrm{mod}(x \cdot y,n)$

Pertanto, si può operare come in $\mathbf{Z}$ e poi ridurre il risultato mod m. Possiamo tuttavia porre alcuni problemi algoritmici:

i) Costruire le tavole di addizione e moltiplicazione mod m.

ii) Determinare quanti e quali sono gli elementi invertibili, costruire la loro tavola di moltiplicazione, trovare i loro inversi.

iii) Risolvere equazioni algebriche negli anelli $\mathbf{Z}_n$.

iv) Trovare applicazioni delle congruenze mod m.

I primi tre problemi si risolvono anche con l'ausilio di software matematico o di linguaggi di programmazione. Un esempio di iv) è costituito dai criteri di divisibilità.

Il termine "congruenza" ha anche altri significati, a seconda dei contesti. Nel seguito ha il significato seguente: dato il numero intero $m > 1$, dati i numeri interi a, b, con $a \neq 0$, trovare x intero tale che $a \cdot x \equiv b \pmod{m}$. Tenuto conto della definizione della relazione di congruenza mod m in $\mathbf{Z}$, deve esistere q intero tale che $a \cdot x - b = m \cdot q$. Posto $y = -q$, si ha l'equazione diofantea $a \cdot x + m \cdot y = b$. Ne segue che b deve essere divisibile per MCD(a, m) e, in tal caso, le soluzioni esistono e sono infinite.

Possiamo tuttavia interpretare la congruenza come una equazione lineare nell'anello $\mathbf{Z}_m$ delle classi di resti mod m. Si pone allora il problema di trovare il numero delle soluzioni in questo ambiente.

Se MCD(a, m) = 1 allora esiste l'inverso moltiplicativo $\bar{a}$ di a, quindi da $a \cdot x \equiv b \pmod{m}$ segue $x \equiv \bar{a} \cdot b \pmod{m}$ e la soluzione in $\mathbf{Z}_m$ è unica.

Supponiamo MCD(a, m) = d. Poniamo a = a'd, m = m'd, b = b'd. Mutatis mutandis, la formula risolutiva delle equazioni diofantee ci dà, per la x:

$$x = x_0 + k \cdot m', \text{ k intero.}$$

Dobbiamo però ridurre mod m. Dividiamo k per d: $k = d \cdot q + r$, con $0 \le r < d$. Sostituiamo:

$$x = x_0 + k \cdot m' = x_0 + (d \cdot q + r) \cdot m' \equiv x_0 + r \cdot m' \pmod{m}.$$

Ci sono pertanto al più d soluzioni distinte $x \equiv x_0 + r \cdot m' \pmod{m}$, $0 \le r < d$.
Ma queste sono tutte soluzioni non congrue mod m, come si prova con il consueto argomento basato sul fatto che d è il minimo intero positivo tale che m'd = m.

ESEMPIO 3.14. Sia data $85x \equiv 50 \pmod{120}$. Poiché MCD(85, 120) = 5, divisore di 50, allora ci sono cinque soluzioni in $\mathbf{Z}_{120}$. Risolvendo l'equazione diofantea 85x+120y=50 troviamo x = 2+24k (sono calcoli già visti, con lo scambio dei ruoli di x ed y). Allora avremo $x \equiv 2 + 24k \pmod{120}$, $0 \le k \le 4$. Quindi la lista delle soluzioni in $\mathbf{Z}_{120}$ è $\{2, 26, 50, 74, 98\}$.

Un altro approccio: semplificando per 5, l'equazione data equivale a

$$17x \equiv 10 \pmod{24}.$$

Poiché MCD(17, 24) = 1, allora 17 ha l'inverso mod 24 e l'inverso è proprio 17 (trovato però per tentativi). Allora $x \equiv 10 \cdot 17 \equiv 170 \equiv 2 \pmod{24}$.
Dunque, x = 2+24k, come sopra.

ESEMPIO 3.15. Vogliamo trovare l'inverso di un elemento x di $\mathbf{Z}_m^*$. Per esempio, vogliamo trovare l'inverso di 17 in $\mathbf{Z}_{28}^*$. Poiché MCD(17,28) = 1, tale inverso esiste. Possiamo procedere in vari modi:
a) eseguire i prodotti mod(x·i,m) per i = 1, ... , m-1, fino a che, per un dato i_0 non si trovi mod(x·i_0,m) = 1. A quel punto, $x^{-1} = i_0$.

x	1	2	3	4	5
17·x	17	6	23	12	1

$\Rightarrow 17^{-1} = 5.$

b) utilizzare l'algoritmo euclideo delle divisioni successive per trovare due numeri u, b tali che x·u + m·v = 1. In tal caso, x^{-1} = mod(u,m). Questo è il metodo di solito nettamente più rapido con numeri grandi.

28	17	11	6	5	1
1	0	1	–1	2	–3
0	1	–1	2	–3	5
		1	1	1	1

$\Rightarrow 28\cdot(-3)+17\cdot 5=1\Rightarrow 17^{-1}=5$

c) poiché $\mathbf{Z}_m^*$ è finito, se $x\in \mathbf{Z}_m^*$ allora esiste $h > 0$, minimo, tale che $x^h \equiv 1 \pmod m$, ossia $\mathrm{mod}(x^h,m) = 1$. Dunque, $x^{-1} = \mathrm{mod}(x^{h-1},m)$.

Ora, h è il periodo di x nel gruppo $\mathbf{Z}_m^*$, che ha $\varphi(m)$ elementi, Dal *teorema di Lagrange*, che vedremo per i gruppi finiti, segue allora che h divide $\varphi(m)$ e quindi $x^{\varphi(m)} \equiv 1 \pmod m$. Ne segue $x^{-1} \equiv x^{\varphi(m)-1} \pmod m$.

Nel nostro caso:

$$\varphi(28)=28\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{7}\right)=12\Rightarrow 17^{-1}\equiv 17^{11}\equiv 5\pmod{28}.$$

Tuttavia, il periodo moltiplicativo di 17 (mod 28), che è un divisore di 12, è in realtà 6. Infatti,

$17^2 = 289 \equiv 9 \pmod{28}$,

$17^3 \equiv 17\cdot 9 = 153 \equiv 13 \pmod{28}$,

$17^4 \equiv 9^2 = 81 \equiv 25 \pmod{28}$,

$17^6 \equiv 13^2 = 169 \equiv 1 \pmod{28}$,

quindi il periodo è 6. Allora $17^{-1} \equiv 17^{6-1} \equiv 5 \pmod{28}$

§ 4 – I NUMERI RAZIONALI

Dalla possibilità di risoluzione dell'equazione a+x = b nasce la nozione di ordine naturale per **N**: si pone a ≤ b se esiste c∈**N** tale che a+c = b, ossia se l'equazione a+x = b ha soluzione. Come abbiamo visto, questa è una relazione d'ordine *totale* per **N**: si ha 0 < 1 < 2 < 3 < ... e non c'è il massimo.

Similmente, dalla possibilità di risoluzione dell'equazione ax = b nasce la nozione di divisibilità in **N**: si pone a | b (a *divide* b) se esiste c∈**N** tale che ac = b, ossia se l'equazione ax = b ha soluzione. Come visto, questa è una relazione d'ordine *parziale* per **N**, in cui 1 è il minimo e 0 è il massimo.

La necessità di risolvere in ogni caso quelle due equazioni ha portato all'esigenza di ampliare l'insieme dei naturali. Il procedimento, applicato ai due monoidi commutativi *regolari* (**N**, +, 0) ed ($\mathbf{N}^+$, ·, 1) (in cui cioè ogni elemento è cancellabile) si chiama *simmetrizzazione* e porta alla costruzione rispettivamente del gruppo additivo degli *interi relativi* (**Z**, +) ed al gruppo moltiplicativo ($\mathbf{Q}^+$, ·) dei *razionali assoluti*.

Prima di accennare a questo procedimento, conviene però osservare che nella scuola elementare tradizionale, da **N** si passa a $\mathbf{Q}^+$ considerando i numeri razionali come *operatori* su grandezze: i 3/4 di un segmento, i 2/5 di una torta (= angolo giro) ecc. L'equivalenza e le operazioni sono definite di conseguenza, mediante il loro effetto sulle grandezze:

3/5 (della torta) + 1/6 (della torta) = (18/30 + 5/30) (della torta) =

=23/30 (della torta);

Questa operazione è analoga all'addizione "punto per punto" tra le funzioni. Analogamente per la moltiplicazione, che è identificabile con la composizione degli operatori.

Successivamente, nella scuola media si passa da $\mathbf{Q}^+$ a **Q** mediante aggiunta dei segni ed estensione delle operazioni, eseguita in modo che si mantengano le loro proprietà. Talvolta nelle scuole superiori, e quasi sempre all'Università, da

N si passa invece all'anello **Z** per simmetrizzazione dell'addizione ed estensione della moltiplicazione, e poi da **Z** a **Q** mediante simmetrizzazione della moltiplicazione ed estensione dell'addizione.

PROPOSIZIONE 4.1. Simmetrizzazione di un monoide commutativo regolare. - Sia $(M, *, 1_M)$ un monoide commutativo regolare. Esistono un gruppo $(G, *)$ ed un suo sottomonoide M', "isomorfo" ad M, tale che per ogni $g \in G$ esistono $a,b \in M'$, tali che $g = a \cdot b^{-1}$.

Dimostrazione. Si consideri il prodotto cartesiano M×M, i cui elementi sono le coppie ordinate (a, b), con $a, b \in M$. Si definisca in M×M la seguente operazione:

$$(a, b)*(c, d) = (a*c, b*d).$$

Non è difficile provare che essa possiede la proprietà associativa ed ha elemento neutro $(1_M, 1_M)$. Si ha così il monoide $(M\times M, *, (1_M, 1_M))$, *prodotto diretto* del monoide dato con se stesso, e che è a sua volta commutativo e regolare.

Si definisca ora in M×M la seguente relazione: $(a, b) \sim (a', b')$ se $a*b' = b*a'$.

Non è difficile provare che ~ è una relazione d'equivalenza in M×M, ossia che possiede le proprietà riflessiva, simmetrica e transitiva.

Si denoti con [a, b] la *classe d'equivalenza* di (a, b), costituita da tutte le coppie equivalenti ad (a, b).

Si tenga presente che se $(a, b) \sim (a', b')$ allora [a, b] = [a', b']; inoltre, due classi distinte hanno sempre intersezione vuota.

A titolo di esempio, consideriamo la coppia $(1_M, 1_M)$: una coppia (c, d) è equivalente ad essa se e solo se $c * 1_M = d * 1_M$, ossia se e solo se c = d.

Pertanto $[1_M, 1_M] = \{(a, a) \mid a \in M\} = [a, a]$ per ogni $a \in M$.

Denotiamo con G l'insieme M×M /~ delle classi, ossia l'*insieme quoziente*.

La proprietà da sottolineare è la seguente: la relazione ~ è *compatibile* con $*$:

$$(a, b) \sim (a', b') \text{ e } (c, d) \sim (c', d') \Rightarrow (a*c, b*d) \sim (a'*c', b'*d').$$

E' allora possibile definire tra le classi la seguente operazione:

$$[a, b] * [c, d] = [a*c, b*d],$$

sicuri che il risultato non dipende dalle particolari coppie prescelte per rappresentare le classi d'equivalenza, ma solo dalle classi stesse.

Si verifica facilmente che questa operazione in G è associativa, commutativa ed ha elemento neutro $[1_M, 1_M]$. Inoltre, ogni classe [a, b] possiede l'inversa: è la classe [b, a], infatti $[a, b] * [b, a] = [a*b, b*a] = [a*b, a*b] = [1_M, 1_M] = 1_G$.

Pertanto, $(G, *)$ è un gruppo abeliano.

Si verifica poi che il sottoinsieme M' costituito dalle classi del tipo $[a, 1_M]$ è un sottomonoide del gruppo G e che M' è isomorfo al monoide M.

Si osservi che ora per ogni $[a, b] \in G$, si ha $[a, b] = [a, 1_M] * [b, 1_M]^{-1}$.

Infine, gli elementi di M' si identificano con quelli di M, cioè, per ogni $a \in M$ si pone $a = [a, 1_M]$.

Ma allora si può scrivere, in G: $[a, b] = a * b^{-1}$.

Nel caso di (**N**, +, 0) la relazione ~ diventa: (a,b) ~ (c,d) se a+d = b+c. L'operazione tra le coppie è: (a,b)+(c,d) = (a+c, b+d). Il suo elemento neutro è la coppia (0, 0). Poiché si sta parlando in termini di addizione, anziché $[b, 0]^{-1}$ si scrive -[b, 0], e questo elemento si denota con -b.

Si ha così che il gruppo quoziente è sostanzialmente il gruppo additivo (**Z**, +) dei numeri interi relativi.

Identifichiamo **N** con il sottoinsieme $\{[n,0] \mid n \in \mathbf{N}\}$ di **Z**. Si ha così la seguente proprietà:

ogni elemento di **Z** o appartiene ad **N** o è l'opposto di un elemento di **N**. (*)

Infatti, dato $[a,b] \in \mathbf{Z}$, se $a \geq b$ si ha [a, b] = [a-b, 0], risultando a+0 = b+(a-b).

Se invece a < b, essendo a+(b-a) = b+0, si ha [a, b] = [0, b-a] = -[b-a, 0].

Pertanto la classe [a,b] può essere denotata con il numero naturale a-b quando $a \geq b$, e con -(b-a) quando a < b. Per esempio, [7, 3] = 4, [6, 8] = -2, ecc.

Questa costruzione di **Z**, pur così astratta, presenta alcuni vantaggi: le definizioni e le dimostrazioni sono dirette e generali e non è necessario esaminare sottocasi. Essa consentirebbe di definire in **Z** anche la moltiplicazione e l'ordinamento, a partire da quelli di **N**, ma non in modo abbastanza elementare. Forse per quest'ultima ragione, come detto, nei testi di Aritmetica della scuola secondaria questa via non viene mai seguita e si preferisce costruire **Z** a partire da **N** mediante l'aggiunta dei segni, via che pur necessita dell'esame di una certa casistica per definire le operazioni, come abbiamo visto.

Nel gruppo (**Z**, +) l'equazione da cui si era partiti, ossia a+x = b, ha sempre una ed una sola soluzione: x = (-a)+b, ovvero x = b-a.

Nel caso del monoide ($\mathbf{N}^+$, ·, 1), le coppie (a, b) di elementi di $\mathbf{N}^+$ sono dette *frazioni* e sono scritte nella forma $\frac{a}{b}$. La relazione ~ è in questo caso: $\frac{a}{b} \sim \frac{a'}{b'} \Leftrightarrow a \cdot b' = b \cdot a'$. L'operazione tra le frazioni è: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$. L'elemento neutro è la frazione $\frac{1}{1}$.

Il gruppo quoziente è il gruppo moltiplicativo $\mathbf{Q}^+$ dei "numeri razionali assoluti" (non nulli). I suoi elementi sono le classi di equivalenza di frazioni $\left[\frac{a}{b}\right]$. L'inverso di $\left[\frac{a}{b}\right]$ è $\left[\frac{b}{a}\right]$.

Il sottomonoide corrispondente ad $\mathbf{N}^+$ è $\left\{\left[\frac{a}{1}\right] \,\middle|\, a \in \mathbf{N}^+\right\}$. Identificando $a \in \mathbf{N}^+$ con $\left[\frac{a}{1}\right]$, si ha $\left[\frac{a}{b}\right] = a \cdot b^{-1}$.

Gli elementi di $\mathbf{Q}^+$ si denotano comunque con $\frac{a}{b}$ anziché con $\left[\frac{a}{b}\right]$ o con ab^{-1}.

Poiché la relazione d'ordine | in $\mathbf{N}^+$ non è totale, non vale in $\mathbf{Q}^+$ una proprietà analoga a (*). Infatti per esempio $\frac{2}{3}$ non è un numero naturale e neppure il reciproco di un numero naturale, sostanzialmente perché 2 non divide 3 e 3 non divide 2.

Nel gruppo ($\mathbf{Q}^+$, ·) l'equazione ax = b da cui siamo partiti (si ricordi che è $a \neq 0$) ha sempre la sola soluzione: $x = a^{-1}b$, cioè $x = b/a$.

Questa costruzione di $\mathbf{Q}^+$ consente, come noto, di definire agevolmente anche l'addizione, dapprima tra le frazioni ponendo $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ e, poiché anche questa operazione risulta compatibile con la relazione d'equivalenza ~, in seguito si estende anche tra le classi di frazioni, cioè tra numeri razionali assoluti.

Aggiungendo poi anche le frazioni $\frac{0}{b}$ (con $b \neq 0$), tutte equivalenti fra loro, il quoziente $\mathbf{N}\times\mathbf{N}^+/\sim$ con l'addizione quoziente è un monoide commutativo regolare, il cui elemento neutro è la classe $0 = \left[\frac{0}{b}\right]$. La simmetrizzazione di tale monoide è il gruppo additivo ($\mathbf{Q}$, +) dei numeri razionali.
Esso diviene infine un campo estendendo convenientemente anche la moltiplicazione di $\mathbf{Q}^+$ mediante le regole dei segni.

Questa via è sostanzialmente seguita nei corsi di Aritmetica della scuola secondaria. E' assai astratta, le dimostrazioni non sono facilissime (ma quasi sempre sono omesse), tuttavia la scrittura $\frac{a}{b}$, cui si è abituati fin dalle scuole elementari, la rende abbastanza accessibile.

Invece, nei corsi universitari, a partire da $\mathbf{Z}$, su cui si sia definita la moltiplicazione in modo da ottenere la struttura di anello, mediante simmetrizzazione del suo monoide moltiplicativo ($\mathbf{Z}\setminus\{0\}$, $\cdot$, 1) ed estensione (in modo opportuno) dell'addizione, si ottiene il campo $\mathbf{Q}$. Questa via presenta vari vantaggi, poiché si applica anche ad altri casi non numerici, tra cui i polinomi, ed è seguita nei corsi universitari. Si chiama: *immersione di un dominio d'integrità nel suo campo dei quozienti*.

Riassumendo: Da $\mathbf{N}$ al campo $\mathbf{Q}$ si va secondo uno dei due itinerari seguenti:

$$\mathbf{N} \xrightarrow{\text{via additiva}} \mathbf{Z} \xrightarrow{\text{via moltiplicativa}} \mathbf{Q}$$
$$\mathbf{N} \xrightarrow{\text{via moltiplicativa}} \mathbf{Q}^+ \xrightarrow{\text{via additiva}} \mathbf{Q}$$

Tra le proprietà di $\mathbf{Q}$ ricordiamo solo quella che riguarda l'ordinamento: tra due numeri razionali distinti x, y, con $x < y$, ce ne sono sempre (infiniti) altri: uno di essi è la *media aritmetica*: $x < \frac{x+y}{2} < y$. Perciò l'ordine di $\mathbf{Q}$ è detto *denso*.

Una costruzione di $\mathbf{Q}$ come *campo dei quozienti* del dominio d'integrità $\mathbf{Z}$ si vedrà in corsi successivi.

§ 4 – I NUMERI REALI

Sia (K, +, ·) un campo. Denotiamo con 0 ed 1 i suoi elementi neutri. Sia poi data in K una relazione d'ordine totale ≤ tale che, per ogni a, b, c∈K si abbia:

a) $a \le b \Rightarrow a+c \le b+c$

b) $\begin{cases} ac \le bc & \text{se } c > 0 \\ ac \ge bc & \text{se } c < 0 \end{cases}$.

La quaterna (K, +, ·, ≤) si dice *campo ordinato.* Un esempio è dato dal campo razionale **Q**.

E' facile provare che per il campo ordinato (K, +, ·, ≤) si ha:

i) $-1 < 0 < 1$

ii) K ha caratteristica 0, quindi contiene il campo razionale.

iii) Posto $K^+ = \{x \in K \mid x > 0\}$, allora K^+ è chiuso rispetto a somma e prodotto e, per ogni $x \neq 0$, fra x e -x uno ed uno solo appartiene a K^+.

Sia ora $\emptyset \neq A \subseteq K$. Un elemento b∈K si dice *maggiorante* di A se per ogni a∈A si ha a ≤ b. Il minimo dei maggioranti, se esiste, è detto *estremo superiore* di A e denotato con sup(A).

Il campo ordinato (K, +, ·, ≤) si dice *completo* se per ogni sottoinsieme non vuoto A che possieda maggioranti esiste in K il sup(A).

Il campo razionale non è completo. Infatti il sottoinsieme $\{x \in \mathbf{Q}^+ \mid x^2 < 2\}$ non ha in **Q** l'estremo superiore.

Si osservi che se sup(A)∉A, allora per ogni ε∈K, ε > 0 esiste un elemento di A tale maggiore di sup(A) - ε, perché altrimenti anche sup(A) - ε sarebbe un maggiorante di A.

Una proprietà equivalente alla completezza è la seguente. Siano A e B due sottoinsiemi di K non vuoti; essi si dicono *separati* se per ogni a∈A e b∈B si ha a ≤ b. Un elemento x_0 tale che $a \le x_0 \le b$ per ogni a∈A e b∈B è detto *elemento di separazione* fra A e B. Il campo ordinato (K, +, ·, ≤) si dice *continuo* se ogni coppia di sottoinsiemi separati ha elementi di separazione in K. Si ha:

- completezza ⇒ continuità: $x_0 = \sup(A)$

- continuità ⇒ completezza: sup(A) = elemento di separazione fra A e qualunque insieme di suoi maggioranti.

In un campo ordinato e completo K vale la seguente proprietà:

TEOREMA 5.1 (Legge di Archimede): per ogni a, b∈K tali che 0 < a < b, esiste n∈**N** tale che na > b.

Dimostrazione. Sia falso. Allora, l'insieme A dei multipli interi na di a possiede b come maggiorante, quindi, per la completezza di K, possiede l'estremo superiore sup(A). Se sup(A) è un multiplo na di a, allora (n+1)a > na, assurdo. Perciò sup(A)∉A.
Allora per ogni ε > 0 esiste un multiplo na di a tale che sup(A)-na < ε. Preso quindi ε ≤ a, si ha (n+1)a = na+a ≥ na+ε ≥ supA, assurdo in ogni caso. Dunque, b non è un maggiorante di A, quindi esiste un multiplo na di a, tale che na > b.

Un *isomorfismo* tra due campi ordinati H e K è una biiezione f:H→K tale che, per ogni a, b∈H, $\begin{cases} f(a+b)=f(a)+f(b) \\ f(a\cdot b)=f(a)\cdot f(b) \\ a\le b \Leftrightarrow f(a)\le f(b) \end{cases}$. In sostanza, due campi isomorfi sono sostanzialmente lo stesso campo scritto con simboli diversi. Si può allora dimostrare la seguente proposizione, di cui non si riporta la dimostrazione:

TEOREMA 5.2. Tutti i campi ordinati completi sono isomorfi tra loro.

Chiamiamo *campo reale* **R** un campo ordinato e completo, che per il teorema precedente è unico a meno di isomorfismi. Questo tuttavia non prova la sua esistenza, ma occorre darne una costruzione. La più classica è quella di **Dedekind**, che chiama *numero reale* ogni *sezione* di **Q**, cioè ogni coppia (A, B) di sottoinsiemi non vuoti e separati di **Q** tali che A∪B = **Q**. Le operazioni sono un poco artificiose, ma non troppo. In questa costruzione i numeri *irrazionali* sono le sezioni (A, B) tali che sup(A) non esiste in **Q**, mentre i numeri razionali corrispondono alle altre sezioni. Nella scuola superiore a volte si fa uso di questa costruzione.

Una costruzione molto elegante, ma assai poco comprensibile, è quella di **Cantor**. Si chiama *successione di Cauchy* ogni successione f in **Q** tale che

$$\forall\, \varepsilon\in\mathbf{Q},\ \varepsilon > 0,\ \exists\ n_\varepsilon\in\mathbf{N} \text{ tale che } |f(n) - f(m)| < \varepsilon\ \forall\ m, n > n_\varepsilon.$$

Si prova che le successioni di Cauchy, con le operazioni *punto per punto*, formano un anello commutativo S. Dato u∈**Q**, una successione di Cauchy f *converge ad u* se

$$\forall\, \varepsilon\in\mathbf{Q},\ \varepsilon > 0,\ \exists\ n_\varepsilon\in\mathbf{N} \text{ tale che } |f(n)-u| < \varepsilon\ \forall\ n > n_\varepsilon.$$

Le successioni convergenti a 0 formano un *ideale massimale* I di S. L'anello quoziente S/I è quindi un campo. Con una opportuna relazione d'ordine, tale campo risulta ordinato e completo e quindi i suoi elementi f+I sono i *numeri reali*. I numeri razionali corrispondono ai laterali f+I, dove f converge ad un u∈**Q**, gli irrazionali sono i laterali di I determinati dalle successioni non convergenti.

Nella scuola media e nelle applicazioni si fa uso della costruzione mediante i numeri decimali e le loro operazioni. Chiamiamo *numero decimale* ogni successione di cifre 0, 1, ... , 9, precedute da un segno + o - e con intercalata una virgola. Un numero decimale x ha quindi la forma:

$$x = x_0,x_1x_2\ldots\ldots, \text{ dove } x_0\in\mathbf{Z} \text{ e } x_i\in\{0, 1, \ldots, 9\} \text{ per ogni } i > 0.$$

Il numero decimale x si chiama *periodico* se esistono r, p > 1 e una sequenza finita di p cifre $a_1a_2\ldots a_p$ tali che

$$x = x_0,x_1x_2\ldots\ldots x_ra_1a_2\ldots a_pa_1a_2\ldots a_pa_1a_2\ldots a_p\ldots\ldots$$

Se p è il minimo intero positivo per cui si ha questa ripetizione, si usa scrivere $x = x_0,x_1x_2\ldots\ldots x_r\,\overline{a_1a_2\ldots a_p}$. In tal caso, il numero naturale $a_1a_2\ldots a_p$ si chiama *periodo* p(x) di x. Il numero naturale $x_0\cdot 10^r+x_1x_2\ldots\ldots x_r$ si dice *antiperiodo* ap(x) di x. Di solito il periodo 0 non si scrive ed il numero si dice *decimale finito.* Ciò posto, diremo *equivalenti* due numeri decimali x ed y se sono periodici e tali che

$$p(x) = 0,\ p(y) = 9,\ ap(x) = ap(y)+1.$$

Per esempio, 32,75 = 32,750000000000..... = 32,7499999.....

Ogni altro numero decimale è posto equivalente solo a se stesso.

Chiamiamo ora *numero reale* ogni classe d'equivalenza di numeri decimali. E' noto che i numeri razionali corrispondono ai decimali periodici. Ma come definire le operazioni?

Siano dati i due numeri razionali x = 1/3 ed y = 12/7. Ad essi possiamo associare i numeri decimali periodici

$$x' = 0{,}333333333333\ldots\ ,\ y' = 1{,}714285714285714285\ldots$$

La loro somma è s = x+y = 43/21, corrispondente ad s' = 2,047619047619047619...

E' possibile ricavare s' da x' ed y' senza ricorrere alle frazioni generatrici?

Consideriamo le due successioni seguenti:

$a_0=0$	$a_1=0{,}3$	$a_2=0{,}33$	$a_3=0{,}333$	$a_4=0{,}3333$	$a_5=0{,}33333$	...
$b_0=1$	$b_1=0{,}4$	$b_2=0{,}34$	$b_3=0{,}334$	$b_4=0{,}3334$	$b_5=0{,}33334$	...

Esse sono formate da decimali finiti tali che per ogni indice $n\in\mathbf{N}$ si ha:

$$a_n \le x' \le b_n \quad \text{e} \quad b_n - a_n = 10^{-n}$$

(l'ordinamento indicato con $\le$ è quello lessicografico solito, corrispondente per altro a quello delle frazioni generatrici. Le operazioni fra decimali finiti si danno per note).

I numeri a_0, a_1, ... si dicono *approssimazioni per difetto* di x' a meno di 10^0 (una unità), 10^{-1} (un decimo), ecc. I numeri b_0, b_1, ... si dicono *approssimazioni per eccesso* di x' a meno di 10^0 (una unità), 10^{-1} (un decimo), ecc.

Ripetiamo ora per y':

$c_0=1$	$c_1=1{,}7$	$c_2=1{,}71$	$c_3=1{,}714$	$c_4=1{,}7142$	$c_5=1{,}71428$	...
$d_0=2$	$d_1=1{,}8$	$d_2=1{,}72$	$d_3=1{,}715$	$d_4=1{,}7143$	$d_5=1{,}71429$	...

Ricordiamo ora la seguente proprietà dei numeri razionali:

$$\text{se } a \le x \le b \text{ e } c \le y \le d \text{ allora } a+c \le x+y \le b+d$$

Pertanto, per ogni $n\in\mathbf{N}$ si ha $a_n+c_n \le s \le b_n+d_n$.

Posto $u_n=a_n+c_n$, $v_n=b_n+d_n$, si ha:

$u_0=1$	$u_1=2{,}0$	$u_2=2{,}04$	$u_3=2{,}047$	$u_4=2{,}0475$	$u_5=2{,}04761$	...
$v_0=3$	$v_1=2{,}2$	$v_2=2{,}06$	$v_3=2{,}049$	$v_4=2{,}0477$	$v_5=2{,}04763$	...

(in grassetto le cifre esatte di s', il quale, ricordiamo, è 2,047619...). In generale u_n e v_n hanno n-1 cifre esatte di s', cioè è incerta solo l'ultima. Si osservi però che nel caso di u_6 e v_6, essendo un 9 la cifra successiva esatta di s', non si ha per il momento la certezza che la cifra 1 sia esatta.
Si ha però $u_7 = \mathbf{2,0476190}$ e $v_7 = \mathbf{2,0476192}$.

Passiamo ora alla moltiplicazione. Sia $p = xy = 4/7$. Il numero decimale corrispondente è p' = 0,571428571428.... Cerchiamo di ricavarlo a partire da x' ed y', osservando che per i numeri razionali positivi si ha:

$$\text{se } 0 \le a \le x \le b \text{ e } 0 \le c \le y \le d \text{ allora } a\,c \le x\,y \le b\,d$$

Pertanto per ogni $n \in \mathbf{N}$ si ha $a_n\, c_n \le p \le b_n\, d_n$. Posto $f_n = a_n c_n$, $g_n = b_n d_n$, si ha (in grassetto le cifre esatte di p'):

$f_0=0$	$f_1=\mathbf{0},51$	$f_2=\mathbf{0,5}643$	$f_3=\mathbf{0,57}07...$	$f_4=\mathbf{0,571}34...$	$f_5=\mathbf{0,5714}2...$
$g_0=2$	$g_1=\mathbf{0},72$	$g_2=\mathbf{0,5}848$	$g_3=\mathbf{0,57}28...$	$g_4=\mathbf{0,571}54...$	$g_5=\mathbf{0,5714}4...$

Di qui si deduce una regola, simile a quella per l'addizione, per ricavare le cifre esatte di p' a partire da quelle di x' ed y'. Anche qui occorre la consueta cautela quando si hanno le cifre 9 e 0.

Regole simili, un poco più complicate, si possono dedurre anche per la sottrazione e la divisione di numeri decimali periodici positivi.

A questo punto è possibile usare queste regole per definire le operazioni anche fra numeri decimali non periodici. Per esempio siano:

x' = 1,71771177711177771111....

y' = 3,012345678910111213141516171819202122232 4... .

Cerchiamo di ricavarne la somma s'. Le successioni sono:

$a_0=1$	$a_1=1,7$	$a_2=1,71$	$a_3=1,717$	$a_4=1,7177$	$a_5=1,71771$	...
$b_0=2$	$b_1=1,8$	$b_2=1,72$	$b_3=1,718$	$b_4=1,7178$	$b_5=1,71772$	...

Pertanto:

$c_0=3$	$c_1=3,0$	$c_2=3,01$	$c_3=3,012$	$c_4=3,0123$	$c_5=3,01234$	...
$d_0=4$	$d_1=3,1$	$d_2=3,02$	$d_3=3,013$	$d_4=3,0124$	$d_5=3,01235$	...

Si ha così, mettendo in grassetto le cifre via via "sicure":

$u_0=4$	$u_1=\mathbf{4},7$	$u_2=\mathbf{4,7}2$	$u_3=\mathbf{4,7}29$	$u_4=\mathbf{4,730}0$	$u_5=\mathbf{4,73005}$ ...
$v_0=6$	$v_1=\mathbf{4},9$	$v_2=\mathbf{4,7}4$	$v_3=\mathbf{4,7}31$	$v_4=\mathbf{4,730}2$	$v_5=\mathbf{4,73007}$ ...

Dunque il numero cercato s' = x'+y' è 4,7300...

Se uno almeno dei due numeri è negativo, per il prodotto si moltiplicano i valori assoluti e si aggiusta il segno con la regola consueta. Per l'addizione si procede come per i numeri interi relativi: a seconda dei segni si sommano o si sottraggono i valori assoluti e si aggiusta poi il segno.

Chiamando con **R** l'insieme dei numeri decimali (positivi e negativi), con le operazioni di addizione e moltiplicazione sopra accennate si ottiene un **campo**, il quale contiene il campo dei numeri decimali periodici, isomorfo al campo **Q** dei numeri razionali. Chiameremo **R** *campo dei numeri reali*.

In **R** l'ordinamento lessicografico, completato al solito modo per i numeri negativi, dà luogo ad un **ordinamento totale** che risulta essere anche **completo**, ossia ogni sottoinsieme non vuoto A di **R**, che ammetta maggioranti, possiede anche l'estremo superiore. Infatti: A ammette anche dei maggioranti interi, e sia b_0 il minimo intero che sia maggiorante di A. Sia poi $a_0 = b_0-1$:

- tra i numeri a_0 $a_0+0,1$ $a_0+0,2$ $a_0+0,3$ ... $a_0+0,9$ $a_0+1 = b_0$, indichiamo con b_1 il più piccolo che sia maggiorante di A e poniamo $a_1 = b_1-0,1$;
- tra i numeri a_1 $a_1+0,01$ $a_1+0,02$ $a_1+0,03$ ... $a_1+0,09$ $a_1+0,1 = b_1$, indichiamo con b_2 il più piccolo che sia maggiorante di A e poniamo $a_2 = b_2-0,01$;
- tra i numeri a_2 $a_2+0,001$ $a_2+0,002$ $a_2+0,003$ .... $a_2+0,009$ $a_2+0,01 = b_2$, indichiamo con b_3 il più piccolo che sia maggiorante di A e poniamo $a_3 = b_3-0,001$;
- ...

Così seguitando, otteniamo una coppia di successioni

$$a_0 \le a_1 \le a_2 \le \dots \le a_n \le \dots, \quad b_0 \ge b_1 \ge \dots \ge b_n \ge \dots$$

di numeri decimali finiti tali che per ogni $n \in \mathbf{N}$ si ha $a_n \leq b_n$ ed inoltre $b_n - a_n = 10^{-n}$. Tale coppia di successioni individua un numero reale x_0 che si prova facilmente essere l'estremo superiore di A cercato.

Per esempio, sia $A = \{x \in \mathbf{R} \mid x > 0 \text{ e } x^2 < 2\}$. Si ha:

$a_0=1$ $a_1=1,4$ $a_2=1,41$ $a_3=1,414$ $a_4=1,4142$ $a_5=1,41421$ ...

$b_0=2$ $b_1=1,5$ $b_2=1,42$ $b_3=1,415$ $b_4=1,4143$ $b_5=1,41422$ ...

Infatti:

$a_0^2 = 1$	$a_1^2 = 1,96$	$a_2^2 = 1,9981$	$a_3^2 = 1,9993...$	$a_4^2 = 1,99996...$
$b_0^2 = 4$	$b_1^2 = 2,25$	$b_2^2 = 2,0164$	$b_3^2 = 2,0022...$	$b_4^2 = 2,00024...$

cosicché il numero x_0 è 1,4142...

Riassumendo, i numeri decimali sono un modello del campo reale. I numeri reali razionali, ossia i decimali periodici, formano a loro volta un campo ordinato isomorfo al campo razionale. Inoltre, **Q** è *denso* in **R**, nel senso che tra due numeri reali qualsiasi distinti c'è sempre un numero razionale, anzi, c'è un decimale finito (che approssima per eccesso il minore e per difetto il maggiore).

§ 6. – I NUMERI COMPLESSI

La formula risolutiva delle equazioni di terzo grado, trovata nel 1500 indipendentemente da Scipione Dal Ferro a Bologna e da Nicolò Fontana (Tartaglia) a Brescia, poi pubblicata da Gerolamo Cardano, nel caso di una equazione con tre soluzioni reali prevede l'estrazione della radice quadrata di un numero negativo. Ciò ha portato all'introduzione dei numeri complessi, studiati da Raffaele Bombelli e dapprima visti come un artificio di calcolo, poi resi "reali" dalla rappresentazione di Gauss e Argand come punti del piano o come vettori. Oggi i numeri complessi sono, nella matematica, l'ambiente naturale di lavoro della geometria algebrica, dell'analisi complessa, delle algebre di Lie, della rappresentazione dei gruppi finiti, ma anche, insospettabilmente, dei software di geometria dinamica, della grafica dei C.A.S. come Derive o della TI-92 e, nell'ingegneria, dei controlli automatici dei processi di lavorazione e dell'elettrotecnica.

Un primo approccio è il seguente: aggiungiamo al campo reale una lettera, solitamente denotata con i, ma anche con j in certe scuole, e postuliamo che valgano le usuali proprietà delle operazioni del calcolo letterale, ma con l'aggiunta della condizione $i^2 = -1$. Allora avremo espressioni del tipo a+ib, con a e b reali. Poiché abbiamo postulato che valgano le usuali proprietà dell'addizione e della moltiplicazione, avremo:

$(a+ib)+(c+id) = (a+c)+i(b+d)$

$(a+ib)(c+id) = ac+iad+ibc+i^2bd = (ac-bd)+i(ad+bc)$

$0 = 0+0i$

$1 = 1+0i$

$-(a+ib) = (-a)+i(-b)$

Inoltre, se a e b non sono entrambi nulli:

$$\frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}$$

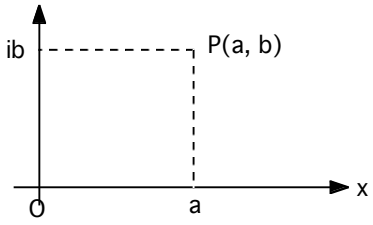
Pertanto, l'insieme di queste espressioni a+ib, con a, b reali, rispetto alle operazioni di addizione e moltiplicazione è un campo, che diremo "campo

complesso" e denoteremo con **C**. Esso contiene il campo reale **R** come "sottocampo", costituito dai numeri complessi a+0i. I numeri del tipo 0+ib, con $b \neq 0$, sono detti numeri immaginari.

Nel campo complesso ogni equazione di II grado ha due soluzioni distinte oppure una doppia. Ma non solo: il *teorema fondamentale dell'algebra* afferma che ogni polinomio di grado $n \geq 1$ ha nel campo complesso almeno una radice e pertanto si scompone in n fattori di primo grado. In particolare, ogni numero complesso ha esattamente n radici n–esime, per ogni $n \geq 2$.

Ma esiste il campo complesso? Ha senso postulare l'esistenza di questa i tale che $i^2 = -1$ e che rispetta le consuete proprietà delle operazioni?

Rappresentazione geometrica dei numeri complessi. Consideriamo il sistema di assi cartesiani ortogonali xOy. L'asse delle x, sul quale rappresenteremo i numeri reali, si chiama *asse dei reali*. L'asse delle ordinate lo chiameremo invece *asse degli immaginari*, perché su di esso rappresenteremo i numeri immaginari: ciascuno di questi ha come immagine il punto che ha per ordinata il coefficiente del numero immaginario.

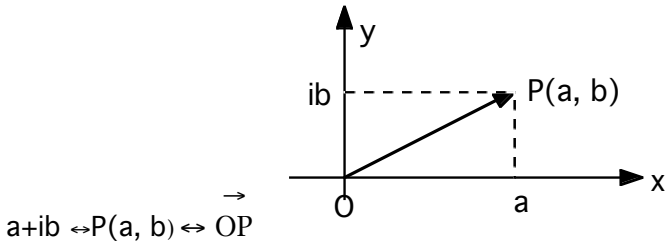


a+ib ↔P(a, b)

Il piano determinato da questi due particolari assi cartesiani si chiama *piano di Gauss-Argand*.

Fra l'insieme dei punti di questo piano e l'insieme dei numeri complessi esiste una corrispondenza biunivoca per cui ad ogni punto del piano corrisponde un determinato numero complesso e, viceversa, ad ogni numero complesso corrisponde un determinato punto del piano, che ha per ascissa la parte reale del numero complesso e per ordinata il coefficiente della parte immaginaria, che si dice *immagine* del numero complesso.

Se poi si considera ogni punto del piano di Gauss-Argand come estremo di un vettore avente come origine il punto origine O dei due assi cartesiani, si può parlare di corrispondenza biunivoca fra i vettori del piano e i numeri complessi.

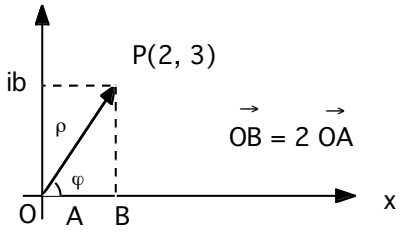


Si può ora rigirare il discorso: definire in $\mathbf{R}^2$ le operazioni nel modo seguente: $(a,b)+(c,d)=(a+c,b+d)$, $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$. Si ottiene certamente un campo. Esso ha un sottocampo costituito dalle coppie (a, 0) e che possiamo identificare con **R**. Ossia, possiamo identificare a con (a, 0). Si ha poi $(0,1)^2=(-1,0)=-(1,0)$ = -1. Posto allora i = (0, 1), si ha:

$(a,b)=(a,0)+(0,b)=(a,0)+(0,1)\cdot(b,0)=a+ib$

e quindi possiamo chiamare **C** questo campo, e ciò ne dimostra l'esistenza.

Tuttavia, se l'addizione dei numeri complessi corrisponde alla somma dei vettori con la regola del parallelogramma, invece, il prodotto non ha una interpretazione geometrica "naturale" e didatticamente appare artificioso.



Relazioni tra i vettori ed i numeri complessi. Sia $\vec{OA}$ il vettore unitario dell'asse dei reali. Consideriamo i numeri reali relativi come operatori che mutano il vettore unitario $\vec{OA}$ in un altro vettore avente la stessa direzione di $\vec{OA}$, lo stesso verso di $\vec{OA}$ o verso contrario a seconda che il numero considerato sia positivo o negativo, e la lunghezza uguale al prodotto della lunghezza di $\vec{OA}$ per il valore assoluto del numero.

Consideriamo l'unità immaginaria i come l'operatore che fa ruotare di 90°, nel verso positivo e intorno alla sua origine, il vettore al quale esso è applicato.

Consideriamo il numero complesso a+ib come l'operatore che fa ruotare il vettore $\vec{OA}$ di un angolo $\varphi = \operatorname{arctg}\frac{b}{a}$ e ne modifica la lunghezza moltiplicando quella di $\vec{OA}$ per $\rho = \sqrt{a^2 + b^2}$.

Si può allora osservare come questo prodotto corrisponda alla composizione di funzioni, applicata agli "operatori" a+ib.

Poiché il triangolo OBP è rettangolo in B, possiamo scrivere:

$$\begin{cases} a = \rho \cdot \cos(\varphi) \\ b = \rho \cdot \operatorname{sen}(\varphi) \end{cases}$$

per cui:

$$a + i\, b = \rho\cdot(\cos\varphi + i \operatorname{sen}\varphi).$$

Questa è la forma trigonometrica dei numeri complessi: ρ si chiama *modulo* e φ si chiama *argomento* del numero complesso a+ib. Tuttavia, l'argomento non è individuato, perché si ha, per ogni k intero:

$$a + i\, b = \rho\cdot(\cos\varphi + i \operatorname{sen}\varphi) = \rho\cdot(\cos(\varphi+2\pi k) + i \operatorname{sen}(\varphi+2\pi k))$$

Mediante le formule di addizione di seno e coseno si ottiene:

$$\rho_1\left(\cos\varphi_1 + i\cdot\operatorname{sen}\varphi_1\right)\cdot\rho_2\left(\cos\varphi_2 + i\cdot\operatorname{sen}\varphi_2\right) = \rho_1\rho_2\left(\cos\left(\varphi_1+\varphi_2\right) + i\cdot\operatorname{sen}\left(\varphi_1+\varphi_2\right)\right)$$

Pertanto, nel prodotto, i moduli si moltiplicano e gli argomenti si sommano. Ciò fa apparire un pò meno artificioso il prodotto di numeri complessi. Si ha poi la *formula di De Moivre* per le potenze:

$$\left(\rho\left(\cos\varphi + i\cdot\operatorname{sen}\varphi\right)\right)^n = \rho^n\left(\cos\left(n\varphi\right) + i\cdot\operatorname{sen}\left(n\varphi\right)\right)$$

che si dimostra per induzione su n, mediante la formula del prodotto.

Altre costruzioni del campo complesso. Una costruzione del campo complesso mediante matrici quadrate d'ordine 2 è la seguente: sia

$\overline{\mathbf{C}} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbf{R} \right\}$. Si verifica subito che questo insieme è chiuso rispetto all'addizione ed alla moltiplicazione di matrici:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}, \quad \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$$

La corrispondenza $a+ib \to \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ tra $\mathbf{C}$ e $\overline{\mathbf{C}}$ è un "isomorfismo", ossia alla somma ed al prodotto di numeri complessi corrisponde la somma ed il prodotto delle corrispondenti matrici di $\overline{\mathbf{C}}$. In particolare, alla "norma" a^2+b^2 di a+ib corrisponde il determinante di $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Al numero complesso reale a+0i corrisponde la matrice "scalare" $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$; all'unità immaginaria i corrisponde la matrice $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, che al quadrato dà $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv -1$.

Quindi, possiamo identificare $\mathbf{C}$ e $\overline{\mathbf{C}}$. Le operazioni sono naturali, perché sono quelle solite fra matrici, ma difficilmente una matrice viene percepita da uno studente generico come un numero, sia pure un po' più generale rispetto ai numeri reali.

Infine, per gli esperti, nell'anello $\mathbf{R}[x]$ dei polinomi nell'indeterminata x ed a coefficienti reali si consideri l'ideale I generato da x^2+1, i cui elementi sono i multipli di x^2+1. Se dividiamo un polinomio f(x) per x^2+1, otteniamo un quoziente q(x) ed un resto r(x) = a+bx, tali che $f(x) = (x^2+1)q(x)+r(x)$. Allora f(x)+I = r(x)+I. Posto i = x+I, ed identificata la costante a con il laterale a+I, si ottiene:

$$a+bi = (a+I)+(b+I)(x+I) = a+bx+I.$$

Pertanto, ogni elemento del quoziente è rappresentabile mediante la scrittura a+ib. Si osservi poi che:

$$i^2 = (x+I)^2 = x^2+I = -1+(x^2+1)+I = -1+I = -1 \ .$$

Le operazioni nell'anello quoziente $\mathbf{R}[x]/I$ si comportano proprio come quelle di $\mathbf{C}$ e quindi abbiamo una costruzione di $\mathbf{C}$ come anello quoziente di

$\mathbf{R}[x]/I$, anello che è un campo, dato che, essendo x^2+1 irriducibile, l'ideale I è massimale e l'anello quoziente è un campo. Questa è a mio avviso la costruzione ottimale di **C**. Ne riparleremo nel capitolo degli anelli.

Il campo complesso non è ordinato. Il campo reale è ordinato, nel senso che ha il sottoinsieme $\mathbf{R}^+$ dei numeri positivi chiuso rispetto a somma e prodotto ed inoltre, per ogni x non nullo, uno ed uno solo fra x e -x è positivo. Posto allora $x<y$ se y-x è positivo, si ha un campo ordinato.

Nell'insieme dei numeri complessi è naturalmente possibile definire ordini totali in tanti modi, ma in nessun caso si può ottenere un sottoinsieme $\mathbf{C}^+$ dei positivi con le stesse proprietà che ha $\mathbf{R}^+$. Infatti, certamente -1 dovrebbe essere negativo, dato che se fosse positivo allora sia $1 = (-1)(-1)$ sia -1 sarebbero positivi, assurdo. Ne segue che -1 è negativo. L'unità immaginaria i com'è? Se fosse positiva, allora $-1 = i^2$ sarebbe positivo a sua volta, assurdo. Allora i dovrebbe essere negativo, quindi -i positivo. Ma anche $(-i)^2 = -1$ lo sarebbe, assurdo. Dunque, il campo complesso non è un campo ordinato.