1. I numeri

1.1. Sistemi numerici

Sia $\mathbb{N}$ un insieme non vuoto, in cui si fissa un elemento detto *zero*, indicato con 0, ed una funzione $+$ da $\mathbb{N}$ in $\mathbb{N}$. Indicata con a^+ l'immagine di a tramite $+$ al variare di $a \in \mathbb{N}$, si dice che a^+ é *elemento successivo*, o *successore*, di a. Si assuma che per l'insieme $\mathbb{N}$ valgano i seguenti assiomi, detti **Assiomi di Peano**:

1. $0 \neq a^+ \ \forall a \in \mathbb{N}$. Ovvero, non esiste alcun elemento di $\mathbb{N}$ avente 0 come successore;
2. La funzione $+$ é iniettiva. Ovvero, non esistono due $a_1, a_2 \in S$ distinti che abbiano uno stesso a^+ come successore;
3. Se $S \subseteq \mathbb{N}, 0 \in S$ e $s^+ \in S \ \forall s \in S$, allora $S = \mathbb{N}$. Ovvero, se S é un sottoinsieme anche improprio di $\mathbb{N}$ che contiene (almeno) 0 e che, per ciascun elemento di S, ne contiene anche l'immagine tramite $+$, allora S e $\mathbb{N}$ sono lo stesso insieme.

L'insieme $\mathbb{N}$ cosí definito prende il nome di **insieme dei numeri naturali**.

Principio 1.1.1 (Principio del buon ordinamento): Sia S un sottoinsieme non vuoto di $\mathbb{Z}$ limitato inferiormente (esiste un $n_0 \in \mathbb{Z}$ tale che $s \geq n_0, \forall s \in S$). Allora S ha minimo, ovvero esiste un $m \in S$ tale che $s \geq m, \forall s \in S$.

Teorema 1.1.1 (Teorema di Ricorrenza): Dati un insieme S, un elemento a di S ed una funzione ϕ da S in sé stesso, esiste una ed una sola funzione $f : \mathbb{N} \to S$ tale che

$$f(0) = a, f(n^+) = \phi(f(n))$$

Principio 1.1.2 (Principio di induzione): Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$ é vera;
- $\forall n$, supponendo che sia vera $P(n)$ é possibile dimostrare che lo sia anche $P(n+1)$.

Allora $P(n)$ é vera $\forall n \in \mathbb{Z}$

Principio di induzione

Si consideri la seguente proposizione, dipendente da n:

$$\sum_{i=1}^{n}(2i-1) = n^2, \forall n \geq 1$$

É possibile applicarvi il principio di induzione ponendo $n_0 = 1$. Nello specifico:

- $P(1)$ é vera. Infatti, $\sum_{i=1}^{1}(2i-1) = (2 \cdot 1) - 1 = 2 - 1 = 1$ e $1^2 = 1$;
- Supponendo che sia vera $P(n)$, si dimostri che é vera $P(n+1)$, ovvero che sia vera $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$. Si ha:

  $$\sum_{i=1}^{n+1}(2i-1) = (2(n+1)-1) + \sum_{i=1}^{n}(2i-1) = 2n+1+\sum_{i=1}^{n}(2i-1) = 2n+1+n^2$$

  Che é peró proprio la formula per il calcolo del quadrato di binomio. Pertanto $n^2+1+2n = (n+1)^2 = \sum_{i=1}^{n+1}(2i-1)$

Essendo verificate entrambe le ipotesi del principio di induzione, si ha che $P(n)$ é vera $\forall n \geq 1$

Il principio di induzione puó essere riespresso in termini diversi.

Principio 1.1.3 (Principio di induzione forte)**:** Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$ é vera;
- $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$.

Allora $P(n)$ é vera $\forall n \in \mathbb{Z}$

L'aggettivo *forte* non sta ad indicare che il principio di induzione forte abbia un maggior potere espressivo del principio di induzione "standard"; indica semplicemente che si basa su una ipotesi (la seconda) piú forte di quella usata dalla formulazione precedente. Infatti, una dimostrazione compiuta mediante una delle due forme del principio di induzione puó essere convertita in una dimostrazione analoga compiuta nell'altra forma.

Teorema 1.1.2: Il principio di induzione, il principio di induzione forte ed il principio del buon ordinamento sono equivalenti.

Dimostrazione: La dimostrazione si compone di tre parti.

1. Assumendo come vero il principio di induzione, si dimostri la validitá del principio di induzione forte. Sia pertanto $P(n)$ una proposizione dipendente da n e sia $n_0 \in \mathbb{Z}$ un valore fissato. Si supponga che siano verificate le seguenti ipotesi:

   - $P(n_0)$ é vera;
   - $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$. In particolare, dunque, se $P(n-1)$ é vera allora $P(n)$ é vera. Il principio di induzione implica quindi che $P(n)$ é vera per ogni $n \geq n_0$;

2. Assumendo come vero il principio di induzione forte, si dimostri la validitá del principio del buon ordinamento. Sia pertanto $S \subseteq \mathbb{Z}$ un sottoinsieme non nullo dei numeri interi inferiormente limitato da n_0. Si supponga per assurdo il principio del buon ordinamento non sia valido, ovvero che S non ammetta minimo. Si consideri la proposizione $P(n)$ dipendente da n:

   $$P(n) = \textit{Non esiste alcun numero intero minore o uguale ad } n \textit{ che appartenga ad } S$$

   É possibile applicare a $P(n)$ il principio di induzione forte. La prima ipotesi é verificata, perché se n_0 appartenesse ad S, essendone il limite inferiore, allora ne sarebbe necessariamente anche il minimo. Sia dunque n un intero maggiore di n_0. Si assuma allora che $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$. Si supponga che $P(n)$ sia falsa: esiste allora qualche $t \leq n, t \in S$. Ma questo non é possibile, perché $\forall t \in \mathbb{Z}, n_0 \leq t \leq n$ si suppone $P(t)$ vera, e quindi $t \notin S$. Occorre allora dedurre che S ammetta minimo, e quindi se si assume come valido il principio di induzione forte allora é valido il principio del buon ordinamento.

3. Assumendo come vero il principio del buon ordinamento, si dimostri la validitá del principio di induzione. Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:

   - $P(n_0)$ é vera;
   - $\forall n$, supponendo che sia vera $P(n)$ é possibile dimostrare che lo sia anche $P(n+1)$.
     Si consideri l'insieme $S \subseteq \mathbb{Z}$ costituito da tutti gli $n \geq n_0$ per i quali $P(n)$ é falsa. Se il principio di induzione fosse verificato, tale insieme dovrebbe essere l'insieme vuoto. Si assuma per assurdo che tale insieme non sia vuoto: per il principio del buon ordinamento tale insieme deve ammettere un minimo, sia questo m, tale per cui $P(m)$ é falsa.

Dato che l'insieme contiene solo interi n tali per cui $n \geq n_0$ (ma non tutti), dovrá aversi che $m > n_0$, ovvero che $m - 1 \geq n_0$. Ma allora $P(m-1)$ deve essere vera, perché altrimenti si avrebbe $m - 1 \in S$ ed m non sarebbe il minimo di S. Applicando la seconda ipotesi sopra definita, si ha che $P(m + 1 - 1) = P(m)$ é vera, ma questo é in contraddizione con quanto evidenziato in precedenza. Occorre allora dedurre che se si assume come valido il principio del buon ordinamento, allora é valido il principio di induzione forte.

□

1.2. Divisione

Dati due numeri interi n e m, con $n > m > 0$, l'operazione di **divisione** permette due interi q e r, chiamati rispettivamente *quoziente* e *resto*, tali che il prodotto fra m e q é il multiplo di m che piú si avvicina ad n per difetto ed il resto $r = n - mq$ misura lo scarto.

Teorema 1.2.1: Siano n e m due numeri interi, con $m \neq 0$. Esiste una ed una sola coppia di interi q ed r tali per cui $n = mq + r$ e $0 \leq r < |m|$

Siano a e b due numeri interi. Se esiste $c \in \mathbb{Z}$ tale che $a = bc$, si dice che b *divide* a, oppure analogamente che a é *divisibile* per b. Per indicare che b divide a viene usata la notazione $b \mid a$. Se b divide a, si dice anche che b é *multiplo* di a. É immediato verificare che, dato $a \in \mathbb{Z}$, sia ± 1 che $\pm a$ sono certamente divisori di a.
Siano $a, b \in \mathbb{Z}$ non entrambi nulli; si dice che $d \in \mathbb{Z}$ é un **Massimo Comun Divisore** tra a e b se sono verificate entrambe le seguenti due condizioni:

1. $d \mid a$ e $d \mid b$. Ovvero, d é divisore sia di a che di b;
2. Se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid d$. Ovvero, tutti i divisori di a che sono anche divisori di b sono anche divisori di d.

Teorema 1.2.2: Dati due numeri $a, b \in \mathbb{Z}$ non entrambi nulli, se d e $\tilde{d}$ sono due Massimi Comun Divisori fra a e b allora devono essere uguali in modulo, ovvero deve aversi $d = \pm\tilde{d}$.

Dimostrazione: Essendo d un Massimo Comun Divisore per a e b, deve valere $d \mid a$ e $d \mid b$. Inoltre, deve valere anche che se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid d$.
Essendo peró anche $\tilde{d}$ un Massimo Comun Divisore per a e b, deve valere $\tilde{d} \mid a$ e $\tilde{d} \mid b$. Allora é possibile sostituire c con $\tilde{d}$ nella seconda espressione ed ottenere che $\tilde{d} \mid d$.
É peró possibile operare anche in senso contrario: essendo $\tilde{d}$ un Massimo Comun Divisore per a e b, deve valere anche che se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid \tilde{d}$, e valendo $d \mid a$ e $d \mid b$ deve aversi che $d \mid \tilde{d}$. Esistono allora due numeri $h, k \in \mathbb{Z}$ tali per cui $\tilde{d} = hd$ e $d = \tilde{d}$. Ne segue $\tilde{d} = (hk)\tilde{d}$, e quindi $hk = 1$. Deve allora aversi $h = k = 1$ e quindi $d = \tilde{d}$ oppure $h = k = -1$ e quindi $d = -\tilde{d}$. □

Dal teorema si evince immediatamente che se d é un Massimo Comun Divisore positivo di due numeri interi a e b, allora d é univoco. Tale valore viene indicato con $\mathrm{MCD}(a, b)$.

Teorema 1.2.3: Per una qualsiasi coppia di numeri interi a e b non entrambi nulli esiste sempre ed é univoco $d = \mathrm{MCD}(a, b)$

Dimostrazione: Innanzitutto, é immediato riconoscere che se $d = \mathrm{MCD}(a, b)$, allora é vero anche $d = \mathrm{MCD}(-a, -b)$. É altrettanto immediato riconoscere che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$ per qualsiasi a, b. Pertanto, senza perdita di generalitá, é possibile assumere che a e b siano numeri naturali con $a \geq b$.
Se $a = 0$ e $b \neq 0$ si verifica facilmente che $\mathrm{MCD}(a, b) = a$; allo stesso modo, se $b = 0$ e $a \neq 0$ si ha $\mathrm{MCD}(a, b) = b$. Si consideri pertanto il caso piú generale in cui $a \neq 0$ e $b \neq 0$. Devono allora esistere un quoziente q_1 ed un resto r_1 tali per cui é possibile eseguire la divisione:

$$a = bq_1 + r_1, 0 \leq r_1 < b$$

Se $r_1 = 0$, allora $\text{MCD}(a, b) = b$, perché $a = bq_1$ é la definizione stessa di $b \mid a$ e q_1 é arbitrario. Se cosí non é, é possibile ripetere l'operazione e risvolgere i calcoli con un nuovo resto ed un nuovo quoziente. Piú in generale:

$$\begin{array}{lll}
(1) & a = bq_1 + r_1 & r_1 \neq 0 \\
(2) & b = r_1q_2 + r_2 & r_2 \neq 0 \\
(3) & r_1 = r_2q_3 + r_3 & r_3 \neq 0 \\
 & \cdots & \\
(k-1) & r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} & r_{k-1} \neq 0 \\
(k) & r_{k-2} = r_{k-1}q_k &
\end{array}$$

Il fatto che prima o poi si giunga ad una k-esima iterazione in cui $r_k = 0$ é garantito dal fatto che tale successione é una successione strettamente crescente di numeri non negativi.
L'ultimo resto non nullo, ovvero r_{k-1}, é precisamente $\text{MCD}(a, b)$. Per verificarlo, é sufficiente osservare come questo possegga entrambe le proprietá enunciate nella definizione di Massimo Comun Divisore:

- Alla riga (k) si ha $r_{k-2} = r_{k-1}q_k$, ovvero $r_{k-1} \mid r_{k-2}$. Sostituendo la riga (k) nella riga $(k-1)$ si ha:

  $$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} = r_{k-1}q_kq_{k-1} + r_{k-1} = r_{k-1}(q_kq_{k-1} + 1)$$

  Ovvero, $r_{k-1} \mid r_{k-3}$ (Si noti come il raccoglimento é ammesso dato che r_{k-1} é definito come non nullo). Risalendo di riga in riga, é facile convincersi che dalla riga (2) si ottiene $r_{k-1} \mid r_1$ e $r_{k-1} \mid b$. Dalla riga (1) segue $r_{k-1} \mid a$. Avendo dimostrato che $r_{k-1} \mid a$ e $r_{k-1} \mid b$, si ha che r_{k-1} possiede la prima proprietá dell'MCD.
- Sia $c \in \mathbb{Z} - \{0\}$. Siano poi $a = c\overline{a}$ e $b = c\overline{b}$. Sostituendo nella riga (1) si ottiene:

  $$a = bq_1 + r_1 \Rightarrow c\overline{a} = c\overline{b}q_1 + r_1 \Rightarrow r_1 = c\overline{a} - c\overline{b}q_1 \Rightarrow r_1 = c\left(\overline{a} - \overline{b}q_1\right)$$

  Da cui si ha $c \mid r_1$. Ponendo $r_1 = c\overline{r_1}$ e sostituendo nella riga (2), si ha:

  $$b = r_1q_2 + r_2 \Rightarrow c\overline{b} = c\overline{r_1}q_2 + r_2 \Rightarrow r_2 = c\overline{b} - c\overline{r_1}q_2 \Rightarrow r_2 = c\left(\overline{b} - \overline{r_1}q_2\right)$$

  Da cui si ha $c \mid r_2$. Discendendo di riga in riga ed applicando lo stesso procedimento, si arriva fino a $c \mid r_{k-1}$. Ma questo equivale a dire che, per un c numero intero generico, se $c \mid a$ e $c \mid b$, allora $c \mid r_{k-1}$, e quindi r_{k-1} possiede anche la seconda proprietá dell'MCD.

□

La dimostrazione del Teorema 1.2.3 fornisce implicitamente anche un algoritmo per calcolare, a partire da due numeri interi a e b non entrambi nulli, il loro MCD. Tale algoritmo prende il nome di **Algoritmo di Euclide**, ed é strutturato come segue:

1. Si calcola qual'é il piú grande intero q tale per cui é possibile moltiplicarlo per b ottenendo un valore inferiore ad a;
2. Si calcola r come differenza fra qb ed a. Se tale valore é nullo, allora q é MCD per a e b, e l'algoritmo termina;
3. q diventa il nuovo a, mentre r diventa il nuovo b. Dopodiché, si torna al punto 1.

Calcolo dell'MCD

L'MCD dei numeri $a = 110143$ e $b = 665$ é 19. Infatti:

$$\begin{aligned}
110143 &= 665 \cdot 165 + 418 \\
665 &= 418 \cdot 1 + 247 \\
418 &= 247 \cdot 1 + 171 \\
247 &= 171 \cdot 1 + 76 \\
171 &= 76 \cdot 2 + 19 \\
76 &= 19 \cdot 4
\end{aligned}$$

Se due numeri interi hanno 1 come Massimo Comun Divisore, allora si dice che tali numeri sono **coprimi** o **primi fra di loro**.

Teorema 1.2.4 (Identitá di Bézout): Se a e b sono due numeri interi non entrambi nulli, allora esistono due numeri interi x e y tali per cui vale:

$$ax + by = \text{MCD}(a, b)$$

Dimostrazione: Facendo riferimento al Teorema 1.2.3, si consideri la successione di operazioni. In particolare, la riga (1), ovvero $a = bq_1 + r_1$, puó anche essere riscritta come $r_1 = a(1) + b(-q_1)$. Sostituendo nella riga (2), si ha:

$$b = r_1q_2 + r_2 \Rightarrow b = (a - bq_1)q_2 + r_2 \Rightarrow r_2 = b - aq_2 + bq_1q_2 \Rightarrow r_2 = a(-q_2) + b(q_1q_2 + 1)$$

In questo modo, é possibile ciascun resto come combinazione lineare di a e di b. In particolare per il resto r_{k-1}, che é anche l'MCD di a e di b, esisteranno due valori x e y tali per cui é possibile esprimerlo come combinazione lineare di a e b, e quindi $r_{k-1} = \text{MCD}(a, b) = ax + by$. □

La definizione di numeri primi fra di loro puó essere riformulata anche rispetto a tale identitá.

Teorema 1.2.5: Due numeri interi a e b sono coprimi fra di loro se e soltanto se esistono due numeri interi x e y tali per cui vale $ax + by = 1$.

Dimostrazione: Il primo verso dell'implicazione deriva direttamente dalla definizione di numeri coprimi. Infatti, due numeri interi a, e b si dicono coprimi se il loro MCD é 1; sostituendolo nell'identitá di Bézout, si ha precisamente $ax + by = 1$.
Ció che manca da dimostrare é il secondo verso, ovvero che se per due numeri interi a e b esistono due numeri interi x e y tali per cui $ax + by = 1$, allora a e b sono coprimi. Si supponga per assurdo che, se esistono x e y, tali per cui $ax + by = 1$, allora a e b non siano coprimi. Questo significa che il loro MCD non é 1, ovvero che $ax + by \neq 1$, ma questo é in contraddizione con l'ipotesi assunta per assurdo. □