Divisione tra numeri interi, M.C.D e m.c.m.

Il seguente fondamentale teorema non sarà dimostrato.

Teorema 1. *(divisione in $\mathbb{Z}$) Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che*

1. $a = bq + r$
2. $0 \leq r < |b|$.

Si dice che q è il **quoziente** e r è il **resto** della **divisione** di a per b. Inotre, si ha:

$$r = 0 \iff b \mid a.$$

Osservazione 1. Si osservi che, fissati $a, b \in \mathbb{Z}$, $b \neq 0$, se non si richiede che *2* del Teorema 1 sia verificata, sono infinite le scritture del tipo *1*. Per esempio, se $a = 27$, $b = 4$, si potrebbe scrivere

$$27 = 4 \cdot 7 - 1 = 4 \cdot (-1) + 31,$$

ma (come ben noto) la divisione tra $a = 27$ e $b = 4$ dà luogo alla scrittura:

$$27 = 4 \cdot 6 + 3$$

e quindi il quoziente della divisione tra $a = 27$ e $b = 4$ è $q = 6$, il resto è $r = 3$.

Osservazione 2. Il Teorema 1 formalizza la divisione usuale quando i due interi a, b, $b \neq 0$ sono numeri naturali; si osservi che non si richiede che sia $a \geq b$, perché, se $a < b$, la divisione si può eseguire, essendo vera l'identità:

$$a = b \cdot 0 + a$$

ovvero il quoziente è 0 e il resto è a, che verifica *2* del Teorema 1: in questo caso si ha $a = 0$, eventualità non esclusa dall'enunciato del Teorema.

Quando uno o entrambi i due numeri interi è negativo, si esegue la divisione operando qualche semplice artificio (indicato, in realtà, nella dimostrazione del Teorema stesso) illustrato nei seguenti esempi.

Esempio 1. Si vuole eseguire la divisione tra $a = -37$ e $b = 15$. Si parte dalla divisione tra 37 e 15:

$$37 = 15 \cdot 2 + 7,$$

da cui segue $-37 = -(15 \cdot 2 + 7)$, che però non fornisce il resto secondo l'enunciato del Teorema 1. Allora:

$$-37 = 15 \cdot (-2) - 7 = 15 \cdot (-2) - 15 + 15 - 7 = 15 \cdot (-2 - 1) + 8 = 15 \cdot (-3) + 8$$

Pertanto il quoziente della divisione tra -37 e 15 è $q = -3$, mentre il resto è $r = 8$.

Esempio 2. L'uguaglianza $-37 = 15 \cdot (-3) + 8$ si usa per eseguire la divisione tra $a = -37$ e $b = -15$. Infatti:

$$-37 = 15 \cdot (-3) + 8 = (-15) \cdot 3 + 8.$$

Dunque il quoziente della divisione tra -37 e -15 è $q = 3$, il resto è $r = 8$.

Esempio 3. Per eseguire la divisione tra $a = 257$ e $b = -11$, si esegue la divisione tra 257 e 11, ottenendo

$$257 = 11 \cdot 23 + 4$$

e quindi

$$257 = (-11) \cdot (-23) + 4$$

ovvero il quoziente è $q = -23$, il resto è $r = 4$.

Definizione 1. Siano $a, b \in \mathbb{Z}$, a, b non entrambi nulli. Si dice *massimo comun divisore* tra a e b un intero $d \in \mathbb{Z}$ tale che

- $d \mid a \quad \wedge \quad d \mid b$
- $\forall d' \in \mathbb{Z}$ tale che $d' \mid a \quad \wedge \; d' \mid b$ si ha $d' \mid d$.

Osservazione 3. Si osserva facilmente che se d è un massimo comun divisore tra a e b, lo è anche tra $-a$ e b, tra a e $-b$, tra $-a$ e $-b$. Inoltre, nella Definizione 1 si richiede che almeno uno tra a e b sia non nullo: se uno dei due è nullo, per esempio $a = 0$, allora b è massimo comun divisore tra a e b. Infatti:

- $b \mid 0 \; \wedge \; b \mid b$
- se $d' \in \mathbb{Z}$ è tale che $d' \mid 0 \; \wedge \; d' \mid b$, allora $d' \mid b$.

Teorema 2. *Siano $a, b \in \mathbb{Z}^*$. Allora esiste un massimo comun divisore d tra a e b. Inoltre esistono due numeri interi x_0 e y_0 tali che*

$$d = ax_0 + by_0 \tag{1}$$

Infine, l'unico altro massimo comun divisore è $-d$.

La (1) si chiama *identità di Bézout*.

Nella dimostrazione del Teorema 2 si usa l'algoritmo delle divisioni successive:

$$a = bq_1 + r_1 \qquad 0 \leq r_1 \leq |b|$$

$$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 \leq r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 \leq r_2$$

$$\vdots$$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \quad 0 \leq r_{n-2} \leq r_{n-1}$$

$$r_{n-2} = r_{n-1} q_n \qquad r_n = 0$$

Si prova che l'ultimo resto non nullo r_{n-1} è massimo comun divisore tra a e b.

Osservazione 4. Siano $a, b \in \mathbb{Z}$, a, b non entrambi nulli. Allora esiste un unico massimo comun divisore positivo tra a e b che si indica con $M.C.D.(a, b)$.

Esempio 4. Si vuole esprime il $M.C.D.(185, 166)$ come combinazione lineare di 185 e di 166, utilizzando l'algoritmo delle divisioni successive

$$\begin{array}{rcll}
185 & = & 1 \cdot 166 + 19 & \Longrightarrow 19 = 185 + 166 \cdot (-1) \\
166 & = & 8 \cdot 19 + 14 & \Longrightarrow 14 = 166 + 19 \cdot (8) \\
19 & = & 1 \cdot 14 + 5 & \Longrightarrow 5 = 19 + 14 \cdot (-1) \\
14 & = & 2 \cdot 5 + 4 & \Longrightarrow 4 = 14 + 5(-2) \\
5 & = & 1 \cdot 4 + 1 & \Longrightarrow 1 = 5 + 4 \cdot (-1) \\
4 & = & 1 \cdot 4 + 0. &
\end{array}$$

Il massimo comun divisore tra 185 e 166 è l'ultimo resto non nullo, ovvero $M.C.D.(185, 166) = 1$. Partendo dalla penultima divisione e operando le opportune sostituzioni, si ha:

$$\begin{array}{rcl}
1 & = & 5 + 4 \cdot (-1) = 5 + (14 + 5 \cdot (-2)) \cdot (-1) = 5 + 14 \cdot (-1) + 5 \cdot 2 \\
& = & 5 \cdot 3 + 14 \cdot (-1) = (19 + 14 \cdot (-1)) \cdot 3 + 14 \cdot (-1) \\
& = & 19 \cdot 3 + 14 \cdot (-3) + 14 \cdot (-1) = 19 \cdot 3 + 14 \cdot (-4) \\
& = & 19 \cdot 3 + (166 + 19 \cdot (-8))(-4) = 19 \cdot 3 + 166 \cdot (-4) + 19 \cdot 32 \\
& = & 19 \cdot 35 + 166 \cdot (-4) = (185 + 166 \cdot (-1)) \cdot 35 + 166 \cdot (-4) \\
& = & 185 \cdot 35 + 166 \cdot (-35) + 166 \cdot (-4) = 185 \cdot 35 + 166 \cdot (-39).
\end{array}$$

Quindi l'identità di Bézout si scrive in questo caso:

$$1 = 185 \cdot 35 + 166 \cdot (-39).$$

Definizione 2. Siano $a, b \in \mathbb{Z}^*$. Si dice *minimo comune multiplo* tra a e b un intero $m \in \mathbb{Z}$ tale che

- $a \mid m \quad \wedge \quad b \mid m$
- $\forall m' \in \mathbb{Z}$ tale che $a \mid m' \quad \wedge \quad b \mid m'$ si ha $m \mid m'$.

Teorema 3. *Siano $a, b \in \mathbb{Z}^*$. Se d è un massimo comun divisore tra a e b, allora $\frac{ab}{d}$ è un minimo comune multiplo tra a e b. Inoltre se m' è un altro minimo comune multiplo tra a e b, allora $m' = -m$.*

Osservazione 5. Co le stesse notazioni del Teorema 3, esiste un unico minimo comune multiplo positivo tra a e b che si indica con $m.c.m.(a, b)$.

Definizione 3. Si dice *equazione Diofantea* un'equazione in $\mathbb{Z}$ nelle incognite x, y della forma

$$ax + by = c \tag{2}$$

dove $a, b \in \mathbb{Z}$, a, b non entrambi nulli. Una soluzione di (2) è una coppia $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ tale che risulti $ax_0 + by_0 = c$.

Teorema 4. *Siano $a, b, c \in \mathbb{Z}$, a, b non entrambi nulli, e sia $d = M.C.D.(a, b)$. Allora si ha:*

1. *l'equazione Diofantea* (2) *ha soluzioni se e soltanto se $d \mid c$*
2. *se* (2) *ha soluzioni, detta (x_0, y_0) una di esse, tutte le altre sono di tipo*

$$(x_0 + \bar{b}h, y_0 - \bar{a}h), \quad h \in \mathbb{Z},$$

dove $\bar{a} = \frac{a}{d}$, $\bar{b} = \frac{b}{d}$.

Dimostrazione. Per provare 1, si osservi preliminarmente che $\bar{a} = \frac{a}{d}$, $\bar{b} = \frac{b}{d}$ sono due numeri interi, poichè d è un divisore di a e di b, e si ha

$$a = \bar{a}d, \quad b = \bar{b}d. \tag{3}$$

Si suppone che (2) ammetta soluzioni: sia (x_0, y_0) una di esse. Sarà allora

$$ax_0 + by_0 = c.$$

In virtù di (3), si ha

$$\bar{a}dx_0 + \bar{b}dy_0 = c$$

da cui

$$d(\bar{a}x_0 + \bar{b}y_0) = c$$

e pertanto esiste $h = \bar{a}x_0 + \bar{b}y_0 \in \mathbb{Z}$ tale che $c = dh$ e quindi $d \mid c$.
Viceversa, sia $d \mid c$: quindi esiste $\bar{c} \in \mathbb{Z}$ tale che $c = \bar{c}d$. Per l'identità di Bezout, esistono $x_1, y_1 \in \mathbb{Z}$ tali che

$$d = ax_1 + by_1. \tag{4}$$

Moltiplicando l'identità (4) per $\bar{c}$ si ha

$$\bar{c}d = \bar{c}ax_1 + \bar{c}by_1,$$

ovvero

$$c = (\bar{c}x_1)a + (\bar{c}y_1)b$$

e dunque, posto $x_0 = \bar{c}x_1, y_0 = \bar{c}y_1$, risulta evidente che la coppia (x_0, y_0) è soluzione di (2).
Ammesso che (3) abbia una soluzione (x_0, y_0), si vuol provare che per ogni $h \in \mathbb{Z}$ $(x_0 + \bar{b}h, y_0 - \bar{a}h)$ è ancora una soluzione di (2). Infatti si ha:

$$a(x_0 + \bar{b}h) + b(y_0 - \bar{a}h) = ax_0 + a\bar{b}h + by_0 - b\bar{a}h = ax_0 + by_0 + \bar{a}d\bar{b} - \bar{b}d\bar{a} = ax_0 + by_0 = c.$$

La dimostrazione del fatto le soluzioni di (2) sono tutte del tipo descritto in 2 viene omessa.

Definizione 4. Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Si dice che p è *primo* se

$$(\forall a, b \in \mathbb{Z})\ (p \mid ab \Longrightarrow (p \mid a\ \vee\ p \mid b).$$

Definizione 5. Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Si dice che p è *irriducibile* se

$$(\forall a \in \mathbb{Z})\ (a \mid p \Longrightarrow (a = \pm 1 \vee\ a = \pm p)).$$

Teorema 5. *Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Allora p è primo se e solo se p è irriducibile.*

Proposizione 1. *Esistono infiniti numeri primi.*

Dimostrazione. Si supponga per assurdo che esistano soltanto h numeri primi

$$p_1, p_2, \ldots, p_h \in \mathbb{N}^*$$

(non è lesivo della generalità considerali positivi). Allora $q = p_1 \cdot p_2 \cdot\ \ldots\ \cdot p_h$ non è un numero primo e non lo è neppure $q+1$, perché $q+1$ non può essere un divisore di q ed è pertanto diverso da ogni p_i, $i = 1, \ldots, h$. Quindi esiste $j = 1, \ldots, h$ tale che $p_j \mid (q+1)$. Però risulta anche $p_j \mid q$ e quindi $p_j \mid (q + 1 - q)$, ovvero $p_j \mid 1$, e quindi $p_j = 1$, il che non può succedere, poichè i numeri primi sono diversi da 1. $\square$

Teorema 6. *(Teorema fondamentale dell'Aritmetica)*
Sia $n \in \mathbb{Z}^*$, $n \neq \pm 1$. Allora esistono s numeri primi $p_1, \ldots, p_s$ e s interi naturali $h_1, \ldots, h_s$ tali che

$$n = p_1^{h_1} \cdot\ \ldots\ \cdot p_s^{h_s}.$$

Questa decomposizione è essenzialmente unica, nel senso che se $q_1, \ldots, q_r$ sono numeri primi e $k_1, \ldots, k_r$ sono interi positivi tali che

$$n = q_1^{k_1} \cdot \cdots \cdot q_r^{k_r}$$

allora $s = r$ ed inoltre si può cambiare l'ordine dei fattori in modo che $q_1 = \pm p_1, \ldots, q_s = \pm p_s$, $h_1 = k_1, \ldots, h_s = k_s$.

Osservazione 6. Siano $n, m \in \mathbb{Z} - \{0, \pm 1\}$. Allora esistono $p_1, \ldots, p_s$ numeri primi, $h_1, \ldots, h_s$, $k_1, \ldots, k_s \in \mathbb{N}$ tali che

$$n = p_1^{h_1} \cdots p_s^{h_s}, \quad m = p_1^{k_1} \cdots p_s^{k_s};$$

cioè i due numeri possono essere fattorizzati usando gli stessi fattori primi, eventualmente elevati a potenza 0. Per esempio,

$$945 = 2^0 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^0 \cdot 17^0, \quad 3366 = 2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \cdot 17.$$

Si può provare che

$$M.C.D.(n, m) = p_1^{min(h_1,k_1)} \cdots p_s^{min(h_s,k_s)},$$

$$m.c.m.(n, m) = p_1^{max(h_1,k_1)} \cdots p_s^{max(h_s,k_s)}.$$

Nell'esempio considerato:

$$M.C.D.(945, 3366) = 2^{min(0,1)} \cdot 3^{min(3,2)} \cdot 5^{min(1,0)} \cdot 7^{min(1,0)} \cdot 11^{min(0,1)} \cdot 17^{min(0,1)},$$

quindi $M.C.D.(945, 3366) = 3^2 = 9$. Inoltre

$$m.c.m.(945, 3366) = 2^{max(0,1)} \cdot 3^{max(3,2)} \cdot 5^{max(1,0)} \cdot 7^{max(1,0)} \cdot 11^{max(0,1)} \cdot 17^{max(0,1)},$$

per cui $m.c.m.(945, 3366) = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 = 353.430$.

Principio d'induzione completa - successioni

Principio d'induzione completa (1^a forma)

Fissato $n_0 \in \mathbb{Z}$, si pone
$$\mathbb{Z}(n_0) := \{x \in \mathbb{Z} \ : \ x \geq n_0\}.$$
Si supponga che $P(n)$ sia una proprietà che ha senso $\forall n \in \mathbb{Z}(n_0)$. Se sono soddisfatte le seguenti due condizioni:

(1) $P(n_0)$ è vera

(2) $(\forall n > n_0,\, P(n)$ vera$) \Longrightarrow P(n+1)$ vera

allora $P(x)$ è vera $\forall x \in \mathbb{Z}(n_0)$

Principio d'induzione completa (2^a forma)

Si supponga che $P(n)$ sia una proprietà che ha senso $\forall n \in \mathbb{Z}(n_0)$. Se sono soddisfatte le seguenti due condizioni:

1. $P(n_0)$ è vera
2. fissato $n > n_0$, $(P(m)$ vera $\forall m \in \mathbb{Z}(n_0),\ n_0 \leq m < n,) \Longrightarrow P(n)$ vera

allora $P(x)$ è vera $\forall x \in \mathbb{Z}(n_0)$.

Definizione 6. Sia $(A, \leq)$ un insieme ordinato. Si dice che $(A, \leq)$ verifica la *proprietà del buon ordinamento di* oppure che è *ben ordinato* se ogni sottoinsieme non vuoto di A che ammette minoranti ammette il minimo.

Osservazione 7. L'insieme $\mathbb{Z}$ con il suo ordinamento naturale $\leq$ è ben ordinato. Si dimostra che questa proprietà è equivalente al Principio di induzione completa.

Seguono alcuni esempi nei quali alcune proprietà vengono dimostrate utilizzando il principio di induzione completa.

Esempio 5. Si vuole verificare che $\forall n \in \mathbb{N}^*$ è vera la seguente identità:
$$\mathcal{P}(n) : 3\sum_{i=1}^{n} 4(i^2 - i + 1) = 4n^3 + \frac{9}{2}n^2 + \frac{7}{2}n$$

È opportuno usare per induzione completa. Si deve provare prima che $\mathcal{P}(1)$ è vera. Infatti:
$$3\sum_{i=1}^{1} 4(i^2 - i + 1) = 3 \cdot 4(1^2 - 1 + 1) = 12;$$
d'altra parte per $n = 1$
$$4n^3 + \frac{9}{2}n^2 + \frac{7}{2}n = 4 \cdot 1^3 + \frac{9}{2}1^2 + \frac{7}{2} = 4 + \frac{9}{2} + \frac{7}{2} = 12$$
e quindi $\mathcal{P}(1)$ è verificata. Bisogna provare ora che supponendo vera $\mathcal{P}(n)$, è vera $\mathcal{P}(n+1)$, ovvero si deve dimostrare l'implicazione
$$\mathcal{P}(n) \ \text{ vera} \Longrightarrow \mathcal{P}(n+1) \ \text{ vera.}$$
Esplicitando la tesi si ha:
$$\mathcal{P}(n+1) : 3\sum_{i=1}^{n+1} 4(i^2 - i + 1) = 4(n+1)^3 + \frac{9}{2}(n+1)^2 + \frac{7}{2}(n+1).$$

Con un calcolo diretto si ha:

$$\begin{aligned} 4(n+1)^3 + \frac{9}{2}(n+1)^2 + \frac{7}{2}(n+1) &= 4(n^3+3n^2+3n+1) \\ &\quad + \frac{9}{2}(n^2+2n+1) + \frac{7}{2}(n+1) \\ &= 4n^3 + \frac{33}{2}n^2 + \frac{49}{2}n + 12. \end{aligned} \tag{5}$$

D'altra parte, usando la proprietà associativa della somma su $\mathbb{N}$, e l'ipotesi d'induzione $\mathcal{P}(n)$

$$\begin{aligned} 3\sum_{i=1}^{n+1} 4(i^2-i+1) &= 3\sum_{i=1}^{n} 4(i^2-i+1) + 3\left(4(n+1)^2-(n+1)+1)\right) \\ &= 4n^3 + \frac{9}{2}n^2 + \frac{7}{2}n + 3(4n^2+8n+4-n-1+1) \\ &= 4n^3 + \frac{9}{2}n^2 + \frac{7}{2}n + 12n^2 + 24n + 12 - 3n \\ &= 4n^3 + \frac{33}{2}n^2 + \frac{49}{2}n + 12, \end{aligned}$$

che coincide con (1).

Esempio 6. Si vuole verificare per induzione completa che $\forall n \in \mathbb{N}$, $n \geq 3$ è vera la disuguaglianza:

$$\mathcal{P}(n) : 2^n > 2n+1.$$

Si deve provare prima che $\mathcal{P}(3)$ è vera. Infatti:

$$2^3 = 8$$

d'altra parte per $n = 3$

$$2n+1 = 7$$

e quindi $\mathcal{P}(3)$ è verificata. Bisogna provare ora che supponendo vera $\mathcal{P}(n)$, è vera $\mathcal{P}(n+1)$, ovvero si deve dimostrare l'implicazione

$$\mathcal{P}(n) \text{ vera} \Longrightarrow \mathcal{P}(n+1) \text{ vera}.$$

Esplicitando la tesi si ha :

$$\mathcal{P}(n+1): \quad 2^{n+1} > 2(n+1)+1 = 2n+3.$$

Tenendo presente l'ipotesi d'induzione e ed il fatto ovvio che $2n+1 > 2$ (visto che sicuramente $n > 4$) si ha:

$$2^{n+1} = 2^n \cdot 2 = 2^n + 2^n > (2n+1) + (2n+1) > 2n+1+2 = 2n+3.$$

In conclusione $2^{n+1} > 2n+3$, che corrisponde a $\mathcal{P}(n+1)$.

Esempio 7. Si vuole verificare per induzione completa che $\forall n \in \mathbb{N}$ è vera

$$\mathcal{P}(n) : 3 \mid n^3 - 4n + 12.$$

$\mathcal{P}(0)$ è vera sicuramente poichè $3 \mid 12$. Bisogna dimostrare l'implicazione

$$\mathcal{P}(n) \text{ vera} \Longrightarrow \mathcal{P}(n+1) \text{ vera}.$$

Si ha

$$\mathcal{P}(n+1) : 3 \mid (n+1)^3 - 4(n+1) + 12. \tag{6}$$

A conti fatti $(n+1)^3 - 4(n+1) + 12 = (n^3 - 4n + 12) + 3n^2 + 3n - 3$. Quindi, usando l'ipotesi d'induzione:

$$\left((3 \mid n^3 - 4n + 12) \ \wedge \ (3 \mid 3n^2 + 3n - 3)\right) \implies 3 \mid (n^3 - 4n + 12) + (3n^2 + 3n - 3),$$

che corrisponde a (6).

Definizione 7. Siano A un insieme, $X \subseteq \mathbb{N}$, entrambi non vuoti. Si dice *successione* di elementi di A un'applicazione $f : \mathbb{X} \to A$. In generale si userà la notazione $a_n = f(n)$, $n \in X$.

Delle volte può essere conveniente definire *ricorsivamente* una succesione:

1. si definisce il primo (o i primi) elementi della successione

2. definito l'elemento $(n-1)$-mo, si definisce l'elemento n-mo, (oppure, definiti tutti gli elementi precedenti si definisce l'n-mo).

Esempi

1. *le potenze*: per ogni $a \in \mathbb{R}$, $n \in \mathbb{N}^*$ si pone:

$$\begin{cases} a^0 = 1 \\ a^n = a^{n-1}a \end{cases}$$

2. *il fattoriale*: per ogni $n \in \mathbb{N}$ si pone:

$$\begin{cases} 0! = 1 \\ n! = (n-1)!n \end{cases}$$

3. *la progressione aritmetica*: per ogni $a, d \in \mathbb{R}$, $d \neq 0$, $n \in \mathbb{N}^*$ si pone:

$$\begin{cases} a_0 = a \\ a_n = a_{n-1} + d \end{cases}$$

si osservi che $\forall n \in \mathbb{N}^*$ la differenza tra a_n e a_{n-1} è sempre d

4. *la progressione geometrica*: per ogni $a, d \in \mathbb{R}^*$, $n \in \mathbb{N}^*$ si pone:

$$\begin{cases} a_0 = a \\ a_n = a_{n-1} \cdot d \end{cases}$$

si osservi che $\forall n \in \mathbb{N}^*$ il rapporto tra a_n e a_{n-1} è sempre d

5. *le torri di Hanoi*: Su una di tre aste sono posti n dischi di diametro crescente dal basso verso l'alto e bisogna spostare gli n dischi su un'altra asta, in modo che assumano la stessa disposizione secondo le seguenti regole:

   1) i dischi vanno spostati uno per volta

   2) un disco di diametro minore non va mai posto al di sotto di un disco di diametro maggiore.

   Il problema è quello di capire qual è il numero minimo di mosse da fare per spostare i dischi da un'asta ad un'altra. Si ottiene la formula ricorsiva:

$$\begin{cases} a_1 = 1 \\ a_n = 2a_{n-1} + 1. \end{cases}$$

6. *i numeri di Fibonacci*:

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = a_{n-1} + a_{n-2}. \end{cases}$$

Questa successione venne introdotta dal mercante italiano Fibonacci (Leonardo Pisano, 1180 circa - 1250) nel suo "Liber Abaci" come soluzione del problema delle coppie di conigli.

Esempio 8. Utilizzando la 2^a forma del principio di induzione completa si dimostra la seguente proprietà dei numeri di Fibonacci:

$$\forall k \in \mathbb{N}^*, n \in \mathbb{N}^* \quad F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

Esempio 9. Utilizzando la 1^a forma del principio di induzione completa si prova che due numeri di Fibonacci successivi sono coprimi, ossia hanno massimo comun divisore 1.

Per le successioni definite per ricorrenza è sempre possibile individuare una formula chiusa, ovvero una formula che descriva direttamente l'n-mo termine della successione. Risulta:

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n-volte}.$$

Inoltre, per come il fattoriale è stato definito si ha:

$$n! = (n-1)!n = (n-2)!(n-1)n = \cdots = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1.$$

Si verifica facilmente che la formula chiusa per la progressione aritmetica è:

$$a_n = a + nd$$

e per la progressione geometrica:

$$a_n = a \cdot d^n.$$

Per quanto riguarda le torri di Hanoi, si può ricavare la formula chiusa osservando che:

$$a_n = 2a_{n-1} + 1 = 2(2a_{n-2} + 1) + 1$$
$$= 4a_{n-2} + 2 + 1 = 4(2a_{n-3} + 1) + 2 + 1$$
$$= 8a_{n-3} + 4 + 2 + 1 = 8(2a_{n-4} + 1) + 4 + 2 + 1$$
$$= 16a_{n-4} + 2^3 + 2^2 + 2^1 + 2^0$$
$$= \sum_{i=1}^{n} 2^{i-1}.$$

Esercizio 1. Provare per induzione completa che

$$\sum_{i=1}^{n} 2^{i-1} = 2^n - 1.$$

In conclusione la formula chiusa per la succesione relativa al gioco delle torri di Hanoi è:

$$a_n = 2^n - 1.$$

La formula chiusa per i numeri di Fibonacci è (senza verifica):

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Il numero $\Phi = \frac{1+\sqrt{5}}{2}$ viene chiamato "rapporto aureo" o "proporzione divina".