

Lemma utile Siano $c, n, m \in \mathbb{Z}$ t.r. $c|n \Leftrightarrow c|m$. Allora, per ogni $x, y \in \mathbb{Z}$, vale: $c|xn+ym$.

D.M. Perche' $c|n \Leftrightarrow c|m$, $\exists k, h \in \mathbb{Z}$ t.c. $n = kc$ e $m = hc$. Dati $x, y \in \mathbb{Z}$,

vale: $xn+ym = x(kc) + y(hc) = xkc + yhc = c(xk+yh) \Rightarrow c|xn+ym$. \square

TEOREMA 9.8 Per ogni scelta di $n, m \in \mathbb{Z}$ non entrambi nulli, esiste ed è unico il MCD (n, m) tra n e m .

D.M. Dobbiamo provare solo l'esistenza (si vede Prop. 9.6 per l'unicità).

Consideriamo l'insieme S definito ponendo

$$S := \{s \in \mathbb{N} \setminus \{0\} \mid s = xn+ym \text{ per qualche } x, y \in \mathbb{Z}\}.$$

$S \neq \emptyset$ in quanto se $x=m$ e $y=-m$, ottengo $s = m^2 - m^2 > 0 \Rightarrow m^2 \in S$.

(Teorema 7.4, p. 20)
grazie al teorema di buon ordinamento dei numeri naturali, S ammette minimo d,

cioè $d := \min(S)$. Proviamo che d soddisfa la prop. (1) e la prop. (2) della Def. 3.5.

Verifichiamo che vale (2). Sia $c \in \mathbb{Z}$ t.c. $c|m$ e $c|m$. Dobbiamo dimostrare che $c|d$.

Poiché $d \in S$, $\exists x, y \in \mathbb{Z}$ t.c. $d = xn + ym$. Grazie al Lemma utile, $c|d$, avendo
vale la prop. (2) della Def. 3.5.

Verifichiamo che d soddisfa (1), ovvero $d|m$ e $d|n$. Dimostriamo che $d|m$.

Eseguiamo la divisione di n per d , ottenendo il quoziente q e il resto r :

$$\begin{cases} n = qd + r \\ 0 \leq r < d \end{cases} \Rightarrow \underline{r = n - qd}$$

Rimane da provare che $r=0$. Supponiamo che $r>0$. Osserviamo che:

$$0 < r = n - qd = n - q(xm + ym) = n - qxm - qym = \\ = (1 - qx)m + (-qy)m.$$

$\Rightarrow r \in S$, $r < d = \min(S)$ IMPOSSIBILE $\Rightarrow r = 0$ ovvero $d|m$.

In modo simile si dimostra che $d|m$. \square

Grazie alla dimostrazione precedente, segue il

Corollario 9.8. Siano $n, m \in \mathbb{Z}$ non entrambi nulli, e sia $d := (n, m)$ il loro MCD.

Allora esistono $x, y \in \mathbb{Z}$ t.c.

$$d = xm + \underline{ym}.$$

Osservazione 9.8

(1) Siano $n, m \in \mathbb{Z}$ non entrambi nulli, esista (n, m) il loro MCD.

Osserviamo che la nozione di divisibilità non dipende dal segno:

$$\begin{aligned} d \mid n &\Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } n = kd \Rightarrow n = (-k)(-d) \Rightarrow -d \mid n \\ &\Downarrow -n = (-k)d \Rightarrow \frac{-d}{\cancel{(-k)}} \mid \cancel{n} \\ &\quad (+k)(-d) \Rightarrow -d \mid -n \end{aligned}$$

Dunque, vale:

$$\underline{(n,m)} = \underline{(-n,m)} = \underline{(n,-m)} = \underline{(-n,-m)} = \underline{(|n|,|m|)}.$$

Inoltre, vale:

$$\underline{(n,m)} = \underline{(m,n)}.$$

(2) Detti n, m come sopra, (n,m) è il massimo (nel senso usuale del " \leq ") dei divisori

comuni di n e m . In simboli, vale: \downarrow t.c.

$$(n,m) = \max \{ c \in \mathbb{Z} \mid c \mid n \wedge c \mid m \}.$$

(3) Per ogni $n \in \mathbb{Z} \setminus \{0\}$, vale

$$(n, 0) = (0, n) = |n|.$$

Infatti, $|n|$ è il massimo dei divisori comuni tra n e 0 , ovvero dei divisori di n .

OSSERVAZIONE 9.9. Dati $n, m \in \mathbb{Z}$ non entrambi nulli, grazie al Lemma utile e al Corollario

9.8, segue che vale la seguente equivalenza:

$$\max \{c \in \mathbb{Z} \mid c \mid n \text{ e } c \mid m\} = (n, m) \stackrel{\text{Corollario 9.8}}{=} x \text{ ntym per qualche } x, y \in \mathbb{Z}.$$

e un numero intero $c \in \mathbb{Z}$ è multiplo d. (n, m) se e solo se esiste x tale che $c = x \text{ ntym}$ per qualche $x, y \in \mathbb{Z}$.

DEF. 9.10 Dati $n, m \in \mathbb{Z}$ non entrambi nulli, diciamo che n e m sono **COPRIMI**, o **PRIMI TRA LORO**, se $(n, m) = 1$.

OSSERVAZIONE 9.17

Siano n, m come sopra. Le seguenti affermazioni sono equivalenti:

$$(1) \quad (n, m) = 1.$$

$$(2) \quad \text{Esistono } x, y \in \mathbb{Z} \text{ t.c. } \underline{x^n + y^m = 1}.$$

DIM. $(1) \Rightarrow (2)$ Grazie al Criterio 9.8, $\exists x, y \in \mathbb{Z}$ t.c. $x^n + y^m = (n, m) = 1$.

(2) \Rightarrow (1) Poché $(n, m) | n \Rightarrow (n, m) | m$, grazie al Lemme utile, $(n, m) | x^n + y^m = 1$

Poiché $(n, m) > 0$, vale: $(n, m) = 1$. \square

ESEMPIO 9.11 Per ogni $n \in \mathbb{Z}$, vale: $(n, n+1) = 1$.

Se $x := -1$ e $y := 1$, allora $x^n + y^{n+1} = -n + n+1 = 1 \stackrel{\text{Oss. 9.11}}{\Rightarrow} (n, n+1) = 1$. \square

Proposizione 9.12 Siano $n, m \in \mathbb{Z}$ con entrambi nulli, e sia $d := (n, m)$. Allora i numeri interi $\frac{n}{d}$ e $\frac{m}{d}$ sono coprimi; ovvero $\left(\frac{n}{d}, \frac{m}{d} \right) = 1$.

DIM. Grazie al Golbalib 3.8, $\exists x, y \in \mathbb{Z}$ t.c. $xn + ym = d > 0$. Dividiamo a destra e a sinistra per d , ottenendo

$$\left[x\left(\frac{n}{d}\right) + y\left(\frac{m}{d}\right) \right] = \frac{xn + ym}{d} = \frac{d}{d} = 1$$

$\frac{xn}{d}$ $\frac{ym}{d}$

Osservazione 9.11 precedente implica che $\frac{n}{d}$ e $\frac{m}{d}$ sono coprimi. \square

Proposizione 7.13 Siano $n, m \in \mathbb{Z}$ t.c. $m \neq 0$ e siano q, r i quoziente ed il resto della divisione di n per m . Allora

$$\{c \in \mathbb{Z} \mid c|n \Leftrightarrow c|m\} = \{c \in \mathbb{Z} \mid c|m \Leftrightarrow c|r\}.$$

In particolare, $(n, m) = \underline{(m, r)}$.

DIM. Si sia $A := \{c \in \mathbb{Z} \mid c|m \wedge c|r\}$ e sia $B := \{c \in \mathbb{Z} \mid c|m + c|r\}$. Ricordando

$$n = qm + r = qm + 1 \cdot r. \text{ Grazie al Lemma utile, se } c \in B, \text{ allora } c \in A \Rightarrow B \subset A.$$

D'altra parte, $r = n - qm = 1 \cdot n + (-q)m$. Dunque, applicando il Lemma utile, se $c \in A$,

$$\text{allora } c \in B \Rightarrow A \subset B \subset A \Rightarrow A = B \Rightarrow (n, m) = \max(A) = \max(B) = (m, r). \quad \square$$

ALGORITMO DI EUCLIDE PER IL CALcolo DEL MCD

Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Vogliamo calcolare (n, m) utilizzando la Prop 7.13 e anche $(n, 0) = |n| \quad \forall n \in \mathbb{Z} \setminus \{0\}$. Poiché $(n, m) = (|n|, |m|)$ e $(n, m) = (m, n)$, possiamo sempre supporre che $n \geq m > 0$. Ad esempio se $n = -28$ e $m = 48$, allora $(-28, 48) = (28, 48) = (48, 28) \Rightarrow$ rinominiamo $n := 48$ e $m := 28$.

ALGORITMO DI EUCLIDE $n = q_1 m + r_1$ $m = q_2 r_1 + r_2$ $r_1 = q_3 r_2 + r_3$ \vdots $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ $r_{k-2} = q_k r_{k-1} + \boxed{r_k}$ $r_{k-1} = q_k r_k + 0$	$\begin{array}{c} (n, m) \\ \downarrow \\ (m, r_1) \\ \downarrow \\ (r_1, r_2) \\ \downarrow \\ (r_2, r_3) \\ \vdots \\ \vdots \\ (r_{k-2}, r_{k-1}) \\ \downarrow \\ (r_{k-1}, r_k) \\ \vdots \\ (r_k, 0) \\ \downarrow \\ r_k \end{array}$	<p>Calcolo $x, y \in \mathbb{Z}$ t.c.</p> $xn + ym = r_k = (n, m)$	$r_1 = n - q_1 m$ $r_2 = m - q_2 r_1$ \vdots $r_k = r_{k-1} - q_k r_k$	SOSTITUZIONE A RIETRASO
		\Rightarrow	$\begin{aligned} r_{k-2} &= r_{k-1} - q_{k-1} r_{k-2} \\ r_{k-1} &= r_{k-2} - q_{k-2} r_{k-3} \\ r_k &= r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k (r_{k-3} - q_{k-1} r_{k-2}) \\ &= (1 + q_k q_{k-1}) r_{k-2} + (-q_k) r_{k-3} = \dots = \\ &= xm + ym. \end{aligned}$	

Eser(17) Calcola $(28, 48)$ e $x_1 y_1$ f.t.c. $x \cdot 28 + y \cdot 48 = (28, 48)$.

SOLUZ. Applichiamo l'alg. d'Euclide a 48 e 28 , assino alle sostituz. a ritroso:

$$\begin{array}{l} 48 = 1 \cdot 28 + 20 \\ 28 = 1 \cdot 20 + 8 \\ 20 = 2 \cdot 8 + 4 \\ 8 = 2 \cdot 4 + 0 \end{array} \quad \left| \begin{array}{l} 20 = 48 - 1 \cdot 28 \\ 8 = 28 - 1 \cdot 20 \\ 4 = 20 - 2 \cdot 8 = 20 - 2(28 - 1 \cdot 20) = \\ = 3 \cdot 20 - 2 \cdot 28 = 3(48 - 1 \cdot 28) - 2 \cdot 28 = \\ = 3 \cdot 48 - 5 \cdot 28 \end{array} \right.$$

Val:

$$(48, 28) = 4 = (3) \cdot 48 + (-5) 28.$$

$$\begin{matrix} " & " \\ x & y \end{matrix}$$