Esercizi. Determinare il massimo comun divisore usando l'algoritmo delle divisioni successive tra

1. 252 e 27

2. 302 e 18

e scrivere l'identità di Bezout.

1. $$\overset{a}{252} = \overset{b}{27}\cdot\overset{q_1}{9} + \overset{r_1}{9}$$ $\quad$ $M.C.D.(a,b) = 9$

$$\overset{b}{27} = \overset{r_1}{9}\cdot\overset{q_2}{3} + \overset{r_2}{0}$$

$$9 = 252 + 27\cdot(-9)$$

$$\boxed{9 = 252\cdot 1 + 27\,(-9)}$$

$$d = a x_0 + b y_0$$

$$x_0 = 1 \qquad y_0 = -9$$

2. $$\overset{a}{302} = \overset{b}{18}\cdot\overset{q_1}{16} + \overset{r_1}{14} \Rightarrow 14 = 302 + 18(-16)$$

$$\overset{b}{18} = \overset{r_1}{14}\cdot\overset{q_2}{1} + \overset{r_2}{4} \Rightarrow 4 = 18 + 14(-1)$$

$$\overset{r_1}{14} = \overset{r_2}{4}\cdot\overset{q_3}{3} + \overset{r_3}{2} \Rightarrow 2 = 14 + 4(-3)$$

$$\overset{r_2}{4} = \overset{r_3}{2}\cdot\overset{q_4}{2} + \overset{r_4}{0}$$

$M.C.D.(302, 18) = 2$

$$2 = 14 + 4(-3) = 14 + (18 + 14(-1))\cdot(-3) = 14\cdot 1 + 18(-3) + 14\cdot 3 =$$

$$= 14\cdot 4 + 18\cdot(-3) = (302 + 18(-16))\cdot 4 + 18\cdot(-3) =$$

$$= 302\cdot 4 + 18\cdot(-64) + 18(-3) = 302\cdot 4 + 18(-67).$$

Identità di Bezout $\qquad 2 = 302 \cdot 4 + 18(-67)$.

Def. Siano $a, b \in \mathbb{Z}^*$. Si dice che m è un minimo comune multiplo fra a e b se

1. $a \mid m \ \wedge \ b \mid m$
2. Se $m' \in \mathbb{Z}$ tale che $a \mid m' \wedge b \mid m'$ allora $m \mid m'$.

Teorema. Siano $a, b \in \mathbb{Z}^*$. Allora $m = \frac{a \cdot b}{d} \in \mathbb{Z}$ è un minimo comune multiplo fra a e b. dove $d = M.C.D.(a,b)$ Inoltre $-m$ è l'unico altro minimo comune multiplo fra a e b.

$$d \mid a \ \wedge \ d \mid b \qquad \frac{a \cdot b}{d} \in \mathbb{Z}$$

$$\Downarrow$$

$$\exists h \in \mathbb{Z} \text{ tale che } a = hd \qquad \frac{a \cdot b}{d} = \frac{h \cancel{d} b}{\cancel{d}} = h \cdot b \in \mathbb{Z}$$

Osservazione. Siano $a, b \in \mathbb{Z}^*$. L'unico minimo comune multiplo fra a e b positivo si indica con $m.c.m.(a,b)$.

$$27, 15 \qquad m.c.m.(27,15) = \frac{\overset{9}{\cancel{27}} \cdot 15}{\cancel{3}} = 135.$$

$$\downarrow$$

$$M.C.D.(27,15) = 3$$

Equazioni Diofantee.

Def Siano $a, b, c \in \mathbb{Z}$ con a e b non entrambi nulli. Si chiama equazione Diofantea l'espressione

$$(1) \quad ax + by = c$$

x, y sono incognite. Risolvere una equazione Diofantea significa verificarne la possibilità (verificare se ha soluzioni intere) e determinare tutte le soluzioni.

Teorema. Siano $a, b, c \in \mathbb{Z}$ con a e b non entrambi nulli. L'equazione Diofantea (1) ha soluzioni se e solo se, posto $d = M.C.D.(a, b)$, risulta $d \mid c$.

$$\underbrace{\exists\ (x_0, y_0) \in \mathbb{Z} \times \mathbb{Z} \text{ soluzione di } (1)}_{a x_0 + b y_0 = c} \iff d \mid c.$$

Se (1) ha soluzione (x_0, y_0), tutte le altre soluzioni sono $(x_0 + \bar{b} h,\ y_0 - \bar{a} h)$ $h \in \mathbb{Z}$, dove

$$\bar{a} = \frac{a}{d} \in \mathbb{Z} \quad \bar{b} = \frac{b}{d} \in \mathbb{Z}.$$

Dim. Supponiamo che (1) abbia una soluzione $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Questo vuol dire che

$$a x_0 + b y_0 = c$$

$$\bar{a} = \frac{a}{d} \Rightarrow \underbrace{a = \bar{a} d}$$

$$\bar{b} = \frac{b}{d} \Rightarrow \underbrace{b = \bar{b} d}$$

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

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

Quindi esiste $h = \bar{a} x_0 + \bar{b} y_0 \in \mathbb{Z}$ tale che

$$c = d h$$

e quindi $d | c$.

Viceversa: supponiamo che $d|c$, allora vogliamo provare che esiste una soluzione di (1).

$d | c \Rightarrow \exists \, \bar{c} \in \mathbb{Z}$ tale che $c = \bar{c} d$

Per l'identità di Bezout esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$d = a x_0 + b y_0.$$

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

$$c = \bar{c}\, a x_0 + \bar{c}\, b y_0$$

poniamo $x_1 = \bar{c}\, x_0 \qquad y_1 = \bar{c}\, y_0$

e si ha

$$c = a x_1 + b y_1$$

vale a dire che (x_1, y_1) è una soluzione di (1).

Supponiamo che (1) ammetta una soluzione (x_0, y_0) e sia $h \in \mathbb{Z}$

$$a(x_0 + \bar{b} h) + b(y_0 - \bar{a} h) =$$

$$a x_0 + a \bar{b} h + b y_0 - b \bar{a} h =$$

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

Tralasciamo la dimostrazione del fatto che tutte le soluzioni sono di questo tipo, ovvero che se (x_1, y_1) è una soluzione di (1), allora esiste $h \in \mathbb{Z}$ tale che $x_1 = x_0 + \bar{b} h$, $y_1 = y_0 - \bar{a} h$.

Esercizi. Risolvere, se possibile, la seguente equazione Diofantea.

$$(2) \qquad \underbrace{\overset{a}{456}\,x + \overset{b}{14}\,y = \overset{c}{12}.}$$

Verifichiamo se esistono soluzioni.

$$\begin{array}{r|l} 456 & 2 \\ 228 & 2 \\ 114 & 2 \\ 57 & 3 \\ 19 & 19 \\ 1 & \end{array} \qquad 14 = \underline{2} \cdot 7$$

$$\bar{a} = \frac{456}{2} = 228 \qquad \bar{b} = \frac{14}{2} = 7$$

$M.C.D.(456,14)=2$ e $2 \mid 12$ per cui esistono soluzioni.

Usiamo l'identità di Bezout relativamente a 456 e 14.

$$\begin{aligned}
\overset{a}{456} &= \overset{b}{14} \cdot \overset{q_1}{32} + \overset{r_1}{8} & &\Rightarrow & 8 &= \underbrace{456 + 14(-32)} \\
\overset{b}{14} &= \overset{r_1}{8} \cdot \overset{q_2}{1} + \overset{r_2}{6} & &\Rightarrow & 6 &= \underbrace{14 + 8(-1)} \\
\overset{r_1}{8} &= \overset{r_2}{6} \cdot \overset{q_3}{1} + \overset{r_3}{2} & &\Rightarrow & 2 &= 8 + 6(-1) \\
\overset{r_2}{6} &= \overset{r_3}{2} \cdot \overset{q_4}{3} + \overset{r_4}{0} & & & &
\end{aligned}$$

$$\begin{aligned}
2 &= 8 + 6(-1) = 8 + \big(14 + 8(-1)\big)(-1) = 8 \cdot \underline{1} + 14(-1) + 8 \cdot \underline{1} = \\
&= 8 \cdot 2 + 14(-1) = \big(456 + 14(-32)\big) \cdot 2 + 14(-1) = \\
&= 456 \cdot 2 + 14(-64) + 14(-1) = 456 \cdot 2 + 14(-65).
\end{aligned}$$

$2 = 456 \cdot 2 + 14 \cdot (-65)$

bisogna moltiplicare per $\bar{c} = \frac{c}{d} = \frac{12}{2} = 6$

$$12 = 456 \cdot 12 + 14 \cdot (-390)$$

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

una soluzione è $(12, -390)$. Tutte le soluzioni:

$$(12 + 7h, -390 - 228h) \qquad h \in \mathbb{Z}$$

$h = 0 \qquad (12, -390)$

$h = -1 \qquad (12 - 7, -390 + 228) = (5; -162)$

$h = 1 \qquad (12 + 7, -390 - 228) = \dots$

si può dividere tutto per 2:

$$\underset{a'}{228} x + \underset{b'}{7} y = \underset{c'}{6} \qquad M.C.D.(228, 7) = 1$$

e si può risolvere l'equazione Diofantea semplificata.

$\underset{a'}{228} = \underset{b'}{7} \cdot \underset{q_1}{32} + \underset{r_1}{4} \quad \Rightarrow \quad 4 = 228 + 7(-32)$

$\underset{b'}{7} = \underset{r_1}{4} \cdot \underset{q_2}{1} + \underset{r_2}{3} \quad \Rightarrow \quad 3 = 7 + 4(-1)$

$4 = 3 \cdot 1 + 1 \quad \Rightarrow \quad 1 = 4 + 3(-1)$

$3 = 1 \cdot 3 + 0$

$$1 = 4 + 3(-1) = 4 + (7 + 4(-1))(-1) = 4\cdot 1 + 7\cdot(-1) + 4\cdot 1$$

$$= 4\cdot 2 + 7(-1) = (228 + 7(-32))\cdot 2 + 7(-1) =$$

$$= 228\cdot 2 + 7(-64) + 7(-1) = 228\cdot \underline{\underline{2}} + 7(-\underline{\underline{65}})$$

Identità di Bezout: $1 = 228\cdot 2 + 7(-65)$

$\bar{c}' = \dfrac{c'}{d'} = \dfrac{6}{1} = 6$ $\qquad 6 = 228\cdot 12 + 7(-390)$

Una soluzione è $(12, -390)$. Tutte le soluzioni

$\bar{a}' = \dfrac{a'}{1} = a' = 228$ $\qquad \bar{b}' = \dfrac{b'}{1} = 7$

$$(12 + 7h, -390 - 228h), \quad h \in \mathbb{Z}.$$