I numeri interi

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

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

Proposizione 1. *Per ogni $a, b, c \in \mathbb{Z}$, $a \neq 0$ si ha:*

1. $a \mid b \Rightarrow (a \mid (-b) \wedge -a \mid b \wedge -a \mid (-b))$
2. $(a \mid b \wedge a \mid c) \Rightarrow a \mid (b \pm c)$
3. se $b \neq 0$ $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$
4. se $b \neq 0$ $(a \mid b \wedge b \mid a) \Rightarrow b = \pm a$
5. $a \mid b \Rightarrow a \mid bc$.

Dimostrazione.

1. Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $a|b$. Allora esiste $q \in \mathbb{Z}$ tale che $b = qa$. Quindi

(1) $$-b = (-q)a \Rightarrow a|(-b)$$

   Inoltre $-a = (-q)b$ e pertanto $-a|b$ da cui, usando (1), $-a|(-b)$.
2. Siano $a, b, c \in \mathbb{Z}$ con $a \neq 0$, $a|b$ e $a|c$. Allora esistono $p, q \in \mathbb{Z}$ tali che $b = pa$ e $c = qa$. Quindi $b \pm c = pa \pm qa = (p \pm q)a$ e pertanto $a|(b \pm c)$
3. Siano $a, b, c \in \mathbb{Z}$ con $a \neq 0$, $b \neq 0$, $a|b$ e $b|c$. Allora esistono $r, s \in \mathbb{Z}^*$ tali che $b = ra$ e $c = sb$. Segue che $c = sb = s(ra) = (sr)a$, da cui certamente $a \mid c$
4. Siano $a, b \in \mathbb{Z}^*$ con $a|b$ e $b|a$. Allora esistono $h, k \in \mathbb{Z}^*$ tali che $b = ha$ e $a = kb$. Segue che $b = ha = h(kb) = (hk)b$ e quindi h e k sono due interi il cui prodotto è 1 e pertanto $h = k = 1$ oppure $h = k = -1$, ovvero $b = \pm a$.
5. Siano Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $a|b$. Allora esiste $q \in \mathbb{Z}$ tale che $b = qa$. Allora $bc = (qa)c = (qc)a$ e dunque $a|bc$.

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

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

Osservazione 1. Dalla Proposizione 1 segue subito 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 per esempio $a = 0$, allora b è massimo comun divisore tra a e b. Infatti $b|b$, $b|0$ e se $d' \in \mathbb{Z}$ è tale che $d'|a$ e $d'|b$, allora $d'|b$.

Teorema 2. *Siano $a, b \in \mathbb{Z}^*$. Allora sicuramente esiste un massimo comun divisore d tra a e b. Inoltre esistono due numeri interi x_0 e y_0 tali che $d = ax_0 + by_0$ (identità di Bézout). Infine, l'unico altro massimo comun divisore è $-d$.*

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

$$\begin{aligned}
a &= bq_1 + r_1 \quad & 0 \leq r_1 \leq |b| \\
b &= r_1q_2 + r_2 \quad & 0 \leq r_2 \leq r_1 \\
r_1 &= r_2q_3 + r_3 \quad & 0 \leq r_3 \leq r_2 \\
&\vdots & \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \quad & 0 \leq r_{n-2} \leq r_{n-1} \\
r_{n-2} &= r_{n-1}q_n \quad & r_n = 0
\end{aligned}$$

Osservazione 2. 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 $M.C.D.(a, b)$.

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

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

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 3. Nella stessa situazione del Teorema 2 esiste un unico esiste un unico minimo comune multiplo positivo tra a e b che si indica con $m.c.m.(a, b)$.

Osservazione 4. In virtù della Definizione 1, per ogni $a, b \in \mathbb{N}^*$, $M.C.D.(a, b)$ è l'estremo inferiore tra a e b rispetto alla relazione d'ordine " | "; d'altra parte, per la Definizione 2 $m.c.m.(a, b)$ è l'estremo superiore tra a e b rispetto alla relazione d'ordine " | ". Si può concludere che l'insieme ordinato $(\mathbb{N}^*, \ | \ )$ è un reticolo. Si osservi inoltre che per ogni $n \in \mathbb{N}$, $n \geq 2$, anche l'insieme ordinato $(D_n, \ | \ )$ è un reticolo, in quanto si prova che per ogni $a, b \in \mathbb{N}^*$, $M.C.D.(a, b) \in D_n$ e $m.c.m.(a, b) \in D_n$

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.

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 $\bar{a} = \frac{a}{d} \in \mathbb{Z}$, $\bar{b} = \frac{b}{d} \in \mathbb{Z}$, 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) $\bar{a}dx_0 + \bar{b}dy_0 = c$ 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).
Fissata una soluzione (x_0, y_0) di (2), 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.

Principio d'induzione completa (1^a forma)

Siano $n_0 \in \mathbb{Z}$, $\mathbb{Z}(n_0) := \{x \in \mathbb{Z} \mid x \geq n_0\}$. Si supponga che $P(n)$ sia una proprietà che ha senso $\forall x \in X(n_0)$. 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 $\forall x \in \mathbb{Z}(n_0)$

Dimostrazione. Sia $X = \{x \in \mathbb{Z}(n_0) \ : \ P(n_0)$ è falsa$\}$. Si deve provare che $X = \emptyset$. Si suppone che sia $X \neq \emptyset$. In tal caso, per il buon ordinamento di $\mathbb{Z}$ esiste $x_0 = minX$ e quindi certamente $P(x_0)$ è falsa. $x_0 \neq n_0$, perchè $P(n_0)$ è vera, e quindi $n_0 < x_0$. Si osservi inoltre che $n_0 \leq x_0 - 1 \notin X$ (perchè $x_0 = minX$) e quindi $P(x_0 - 1)$ è vera. Allora, per (2), $P(x_0)$ è vera e ciò costituisce una contraddizione.

Principio d'induzione completa (2^a forma)

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

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

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

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

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

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

Proposizione 2. *Esistono infiniti numeri primi.*

Proof. Si supponga per assurdo che esistano soltanto h numeri primi $p_1, p_2, \ldots, p_h \in \mathbb{N}^*$. 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 $p_j | (q+1)$. Però risulta anche $p_j | q$ e quindi $p_j | (q+1-q)$, ovvero $p_j | 1$, e quindi $p_j = 1$, il che non può succedere, poichè i numeri primi sono diversi da 1. □

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

$$n = q_1^{k_1} \ldots q_r^{k_r}$$

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 5. 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

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

Nel caso 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 $M.C.D.(945, 3366) = 3^2 = 18$. 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 $m.c.m.(945, 3366) = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 = 353430$.