Esercizi

1) Si provi, per induzione su n, che se $x_1,x_2,\ldots,x_n \in \mathbf{Z}$, allora

$$|x_1+x_2+\ldots+x_n| \leqslant |x_1|+|x_2|+\ldots+|x_n|.$$

2) Si trovino quoziente q e resto r della divisione di $a=630$ per $b=-132$. Lo stesso per $a=-71$, $b=36$.
3) Come si modificano q ed r se a,b si sostituiscono con i multipli ma,mb?
4) Si trovino tre interi a,b,c tali che $a \nmid b$, $a \nmid c$, $a \mid bc$.

§ 8. Massimo comune divisore

8.1. Un intero d si dirà un *massimo comune divisore* (brevemente M.C.D.) degli interi a,b (non entrambi nulli) se e solo se

1) d divide entrambi: $d \mid a$, $d \mid b$;
2) d è multiplo di ogni intero che divida entrambi:

$$\text{se } z \mid a,\ z \mid b, \quad \text{allora } z \mid d.$$

Ad esempio -8 è un M.C.D. di 24 e -32. Infatti, osservato che i divisori comuni di 24 e -32 sono: ± 1, ± 2, ± 4, ± 8, si verifica che fra i divisori comuni di 24 e -32 c'è -8 e che tutti i divisori comuni dividono -8. Notiamo che alle medesime condizioni soddisfa il numero 8, ma nessun altro intero. Questo fatto è del tutto generale: se d, d' sono due M.C.D. di a,b, allora la condizione 1) per d' e la condizione 2) per d comportano $d' \mid d$ e scambiando i ruoli otteniamo $d \mid d'$. Ma allora per 7.5. otteniamo $d=d'$ oppure $d=-d'$. *In conclusione possiamo sempre scegliere un* M.C.D. *positivo*: questo particolare M.C.D. di a,b si denoterà con il simbolo (a,b). Visto così che (a,b) *se esiste, è unico*, rimane da vedere che *esiste*. Per dimostrare l'esistenza consideriamo l'insieme $S=\{s \mid s=ax+by;\ x,y \in \mathbf{Z},\ s>0\}$, cioè la totalità degli interi positivi della forma $ax+by$. Poiché a,b non sono entrambi nulli, S non è vuoto, e perciò contiene un elemento minimo $d=at+bs$. Proviamo che risulta $d=(a,b)$. Dividendo a per d scriviamo $a=dp+r$, $0 \leqslant r<d$. Allora $r=a-dq=a-(at+bs)q=a(1-tq)+b(-sq)$. Dunque r è del tipo $ax+by$; se fosse $r>0$ sarebbe $S \ni r<d$, in contrasto con la minimalità di d. Ne segue $r=0$ e quindi $d \mid a$. Analogamente $d \mid b$, e la condizione 1) per il M.C.D. è soddisfatta. Quanto alla 2) si osservi che $z \mid a$, $z \mid b$ comportano $a=zc_1$, $b=zc_2$ e quindi

$$d=at+bs=zc_1t+zc_2s=z(c_1t+c_2s) \quad \text{ossia } z \mid d.$$

8.2. Algoritmo di Euclide. Diamo ora un procedimento di calcolo che permette l'effettiva determinazione di (a,b). Osserviamo intanto che nelle ultime righe abbiamo incidentalmente dimostrato che se $z \mid a$, $z \mid b$, allora $z \mid ax+by$ per ogni $x,y \in \mathbf{Z}$.

Si debba calcolare, ad esempio, (72,22). Dividiamo successivamente 72 per 22, poi 22 per il resto, il primo resto per il secondo resto e così via, fino a ottenere resto 0.

$$\begin{aligned} 72 &= 22\cdot 3+6 \\ 22 &= 6\cdot 3+4 \\ 6 &= 4\cdot 1+2 \\ 4 &= 2\cdot 2+0 \end{aligned}$$

Affermiamo che l'ultimo resto positivo è il M.C.D.: $(72,22)=2$; infatti, leggendo le divisioni precedenti dall'ultima alla prima, e tenendo conto della osservazione preliminare, si ottiene: $2 \mid 4$; $2 \mid 6$ perché $2 \mid 2$, $2 \mid 4$; $2 \mid 22$ perché $2 \mid 4$, $2 \mid 6$; $2 \mid 72$, perché $2 \mid 6$, $2 \mid 22$. Allora il numero 2 soddisfa alla condizione 1) per il M.C.D.. Inoltre se $z \mid 72$, $z \mid 22$, leggendo le divisioni dalla prima all'ultima, si ottiene rispettivamente: $z \mid 6$ perché $6=72\cdot 1+22(-3)$, $z \mid 72$, $z \mid 22$; $z \mid 4$ perché $z \mid 22$, $z \mid 6$; $z \mid 2$ perché $z \mid 6$, $z \mid 4$. E la condizione 2) è provata.

Osserviamo che l'algoritmo euclideo è applicabile ad ogni coppia a,b di interi non entrambi nulli (si incomincerà col dividere a per b, oppure b per a) quindi fornisce un'ulteriore dimostrazione dell'esistenza del M.C.D.. Anzi, l'algoritmo risolve il problema di determinare gli interi t,s che in 8.1. fornivano $d=at+bs$. Infatti utilizzando le divisioni precedenti, dall'ultima alla prima, otteniamo:

$$\begin{aligned} 2 &= 6+4(-1)=6+(22+6(-3))(-1)=22(-1)+6(1+(-3)(-1))= \\ &= 22(-1)+(72+22(-3))4=22(-13)+72(4). \end{aligned}$$

Si è trovato dunque $t=-13$, $s=4$.

8.3. Due numeri interi si dicono *primi tra loro* (sinonimo: *coprimi*) se il loro M.C.D. è l'unità. Le considerazioni precedenti forniscono il seguente