criterio: *due interi a,b sono coprimi se e soltanto se* $1 = ax + by$ *per opportuni interi* x,y. Sia, ad esempio, $b = a + 1$; allora $1 = b - a = a(-1) + b(1)$ e quindi $(a,b) = 1$. Altra applicazione: dividendo due interi a,b per il loro M.C.D. si ottengono due numeri coprimi. Infatti se $a = (a,b)a_1$ e $b = (a,b)b_1$ dalla relazione $(a,b) = ax + by = (a,b)a_1x + (a,b)b_1y$ si ottiene, semplificando per (a,b), $1 = a_1x + b_1y$.

8.4. Un'importante proprietà dei numeri primi è la seguente: *se un primo divide un prodotto, allora esso divide uno dei fattori*. Si otterrà questo risultato come caso particolare del seguente lemma:

$$\textit{se } c \mid ab \textit{ e } (a,c) = 1, \textit{ allora } c \mid b.$$

Dimostrazione: Sappiamo che $1 = cx + ay$ per opportuni $x,y \in \mathbf{Z}$. Moltiplicando per b otteniamo $b = cbx + aby$. Ma, per ipotesi $ab = cz$ per qualche $z \in \mathbf{Z}$, quindi $b = c(bx + zy)$, ossia $c \mid b$. In particolare:

$$\textit{se } p \textit{ è primo allora } p \mid ab \textit{ implica } p \mid a \textit{ oppure } p \mid b.$$

Dimostrazione: Per definizione i divisori di p sono soltanto ± 1 e $\pm p$. Se allora $p \nmid a$, i divisori comuni di p ed a sono ± 1. Allora $(p,a) = 1$ e si applica il lemma precedente.

Osserviamo infine che *se* $a \mid m$, $c \mid m$, *e* $(a,c) = 1$, *allora* $ac \mid m$.

Dimostrazione: Per ipotesi $m = ab$ per qualche b; per il lemma precedente $c \mid b$ ossia $b = cz$ ed infine $m = ab = acz$.

8.5. Diciamo che m è un *minimo comune multiplo* (brevemente: m.c.m.) degli interi a,b (non entrambi nulli) se e solo se

1) m è multiplo di entrambi: $a \mid m$, $b \mid m$;
2) m è divisore di ogni intero che sia multiplo di entrambi:

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

Ad esempio, 96 è un m.c.m. di 24 e -32: la 1) è subito verificata, ma la 2) si prova meno facilmente. Dimostriamo perciò un teorema che riconduce il calcolo del m.c.m. a quello del M.C.D. Osserviamo anzitutto che il m.c.m. è individuato a meno del segno: la dimostrazione è pressoché identica all'analoga per il M.C.D. Dopodiché si indicherà con il simbolo $[a,b]$ il m.c.m. non negativo dei numeri a,b. Il teorema che segue fornisce ad un tempo la dimostrazione dell'esistenza ed un metodo di calcolo.

$$\textit{Se } a,b \in \mathbf{Z}, \textit{ allora } (a,b)\,[a,b] = |ab|.$$

Dimostrazione: Dividendo ab per (a,b) otteniamo evidentemente resto 0:

$ab = (a,b)q$. Si tratta di provare che q soddisfa alle condizioni 1) e 2) della definizione di m.c.m.. Scriviamo infatti $a = (a,b)a_1$ e $b = (a,b)b_1$. Moltiplicando rispettivamente per b e per a otteniamo:

$$(a,b)q = ab = (a,b)a_1b = (a,b)ab_1.$$

Semplificando si ottiene la 1): $q = a_1b = ab_1$. Quanto alla 2), se $a \mid z$, $b \mid z$ possiamo scrivere $z = (a,b)z_1$. Si trova, come prima: $a_1 \mid z_1$, $b_1 \mid z_1$. Poiché a_1, b_1 sono coprimi (cfr. 8.3.), l'osservazione prima di 8.5. fornisce $a_1b_1 \mid z_1$ cosicché $q = a_1b = a_1b_1(a,b)$ divide $z = z_1(a,b)$ e dunque la 2) è verificata.

8.6. La nozione di M.C.D. si estende facilmente a più di due numeri: l'intero d si dice un M.C.D. degli interi $a_1,a_2,\ldots,a_n$ (non tutti nulli) se

1) d divide ciascun a_i $(i = 1,2,\ldots,n)$;
2) d è multiplo di ogni intero che divida ciascun a_i $(i = 1,2,\ldots,n)$.

L'esistenza si può dimostrare ricorrendo al minimo dell'insieme $S = \{s \mid s = a_1x_1 + a_2x_2 + \ldots + a_nx_n;\ x_i \in \mathbf{Z};\ s > 0\}$ e procedendo in modo analogo a quanto abbiamo fatto al paragrafo 8.1. Il M.C.D. risulta ancora individuato a meno del segno e se ne indica con $(a_1,a_2,\ldots,a_n)$ il valore positivo. Si dimostra che risulta $(a_1,a_2,\ldots,a_n) = (a_1,a_2,\ldots,a_{n-1}),a_n)$ (si svolga l'esercizio 3 e si applichi l'induzione su n), e quindi anche il M.C.D. di più di due numeri si può calcolare con successive applicazioni dell'algoritmo di Euclide.

Anche il m.c.m. $[a_1,a_2,\ldots,a_n]$ si può definire per analogia. Per provare l'esistenza di un m.c.m., invece di parafrasare l'8.5., conviene ricorrere al minimo dell'insieme $S = \{s \mid s \in \mathbf{Z},\ s \geq 0,\ a_i \mid s \text{ per ogni } i = 1,2,\ldots,n\}$.

Lasciamo agli esercizi i dettagli.

Esercizi

1) Si calcoli, con procedimento delle divisioni successive, (630,132).
2) Si trovino $s,t \in \mathbf{Z}$ tali che $1 = 54\,s + 19\,t$. Sono s,t individuati da questa condizione?
3) Si dimostri che $(a,b),c) = (a,b,c,) = (a,(b,c))$ per ogni $a,b,c \in \mathbf{Z}$.