Ancora sul massimo comune divisore

Nella visione euclidea, ciò che noi oggi intendiamo con $\mathrm{MCD}(100,6)=2$, corrisponde alla considerazione geometrica secondo cui 2 è la massima lunghezza di un righello (non graduato) che consenta di misurare esattamente due segmenti di lunghezze 100 e 6 rispettivamente. Naturalmente, questa sarà anche la lunghezza massima che consenta di misurare entrambi i seguenti segmenti:

- il segmento di lunghezza minore (6);
- il segmento *residuo* ottenuto sottraendo, dal maggiore, un certo numero di volte quello minore $(100-16\cdot 6=4)$.

Ragionando in termini algebrici, possiamo affermare che, dati, in anello commutativo unitario A, gli elementi x,y,s,t tali che

$$x=ys+t,$$

vale la seguente uguaglianza tra insiemi:

$$\{\text{divisori comuni di } x \text{ e } y\}=\{\text{divisori comuni di } y \text{ e } t\}$$

In effetti: se $a\in A$ è tale che $a|x$ e $a|y$, allora $a|ys$, ma si ha anche $a|t$, in quanto $t=x-ys$. Per l'inclusione opposta ci basterà osservare che se $a|y$ e $a|t$, allora $a|x$, in quanto a divide entrambi gli addendi a secondo membro dell'uguaglianza di sopra. Se $A=\mathbb{Z}$, ciò implica che

$$\mathrm{MCD}(x,y)=\mathrm{MCD}(y,t).$$

In particolare, nell'algoritmo delle divisioni successive

$$\begin{array}{rl}
1) & a=bq_1+r_1\\
2) & b=r_1q_2+r_2\\
\vdots & \\
i) & r_{i-2}=r_{i-1}q_i+r_i\\
\vdots & \\
n-1) & r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}\\
n) & r_{n-2}=r_{n-1}q_n+0
\end{array}$$

si avrà

$\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r_1) = \mathrm{MCD}(r_1,r_2) = \cdots = \mathrm{MCD}(r_{i-1},r_i) = \cdots = \mathrm{MCD}(r_{n-2},r_{n-1}) = \mathrm{MCD}(r_{n-1},0)$,

e quindi, in sintesi,

$\mathrm{MCD}(a,b) = r_{n-1}$.

In generale, in ogni riga dell'algoritmo, si considera che

$$\mathrm{MCD}(\text{dividendo, divisore}) = \mathrm{MCD}(\text{divisore, resto}).$$

Ecco una breve dimostrazione del fatto che l'algoritmo fornisce il risultato desiderato.