# § 9. Fattorizzazione unica

**9.1.** TEOREMA FONDAMENTALE DELL'ARITMETICA: *ogni intero maggiore di* 1 *si può esprimere come prodotto di numeri primi positivi. Questa espressione è unica a meno dell'ordine in cui compaiono i fattori.*

*Dimostrazione*: Proviamo anzitutto l'esistenza di una tale fattorizzazione. Supponiamo, per assurdo, che esistano interi $>1$ che non si lasciano esprimere come prodotto di primi, e sia $m$ il minimo di essi. Allora $m$ non è primo, e quindi ammette divisori diversi da $\pm 1$, $\pm m$; dunque, per opportuni $q,n>1$, risulta $m=nq$. Ma allora $n,q$ sono minori di $m$, e quindi, per la minimalità di $m$, essi si esprimono come prodotti di primi: $n=p_1p_2\cdots p_r$, $q=p'_1p'_2\cdots p'_s$. Si ottiene $m=p_1p_2\cdots p_rp'_1p'_2\cdots p'_s$, una contraddizione. Concludiamo che per ogni $n>1$ si ha $n=p_1p_2\cdots p_t$ per opportuni primi positivi $p_i$.

Quanto all'unicità, supponiamo che sia anche $n=p'_1p'_2\cdots p'_u$ una fattorizzazione in primi positivi. Allora $p_1$ divide $n=p'_1(p'_2\cdots p'_u)$. Per quanto si è visto in 8.4., $p_1 \mid p'_1$ oppure $p_1 \mid (p'_2\cdots p'_u)$. Nel primo caso $p_1=p'_1$ (perché si tratta di primi positivi); nel secondo caso si trova $p_1 \mid p'_2$ oppure $p_1 \mid (p'_3\cdots p'_u)$. Così procedendo si arriva a trovare $p_1=p'_j$ per qualche $j\leqslant u$. I fattori primi si possono riordinare in modo che $p'_j$ sia al primo posto ($j=1$); allora $n=p_1p_2\cdots p_t=p_1p'_2\cdots p'_u$ da cui $p_2p_3\cdots p_t=p'_2p'_3\cdots p'_u$. Si ripete il procedimento fintantoché non si esauriscono i fattori $p_i$. Allo stesso tempo si devono esaurire i $p'_j$. Si conclude che nelle due fattorizzazioni compare lo stesso numero di fattori ($t=u$), anzi compaiono i medesimi fattori primi, al più disposti in ordine diverso.

**9.2.!** Nella fattorizzazione di $n$ il medesimo primo può comparire più volte. È conveniente riordinare i fattori in modo da ravvicinare i primi eguali. Allora, se $p_1,p_2,\ldots,p_v$ sono i fattori primi distinti nella fattorizzazione di $m$, si scrive $m=p_1^{n_1}p_2^{n_2}\cdots p_v^{n_v}$ e gli interi positivi $n_1,n_2,\ldots,n_v$ sono individuati univocamente da $m$. Con riferimento a vari problemi di divisibilità, è conveniente scrivere tutti i numeri in questione (che supporremo per semplicità



positivi) $a,b,\ldots$ come prodotti di potenze dei medesimi numeri primi (distinti): $a=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$; $b=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ ecc. Ciò è sempre possibile purché si ammettano valori nulli per gli esponenti $m_i,n_i$ ecc.

**9.3.** L'unicità della fattorizzazione ci garantisce che, facendo uso di questa *rappresentazione* per $a,b$, risulta $a \mid b$ se e solo se $m_i\leqslant n_i$ per ogni $i=1,2,\ldots,t$. Questa osservazione sta alla base del metodo tradizionale di calcolo del M.C.D.: $(a,b)=p_1^{w_1}p_2^{w_2}\cdots p_t^{w_t}$ *ove* $w_i$ è il minimo tra $m_i$ e $n_i$. Inoltre $[a,b]=p_1^{z_1}p_2^{z_2}\cdots p_t^{z_t}$ ove $z_i$ è il massimo fra $m_i$ e $n_i$.

**9.4.** Ecco una classica applicazione del teorema fondamentale: *Esistono infiniti numeri primi.*

*Dimostrazione* Se infatti i primi fossero in numero finito: $p_1,p_2,\ldots,p_t$ allora il numero $m=p_1p_2\cdots p_t+1$ sarebbe coprimo con $p_1p_2\cdots p_t$ (cfr. 8.3), e dunque con ogni primo $p_i$. Ma allora $m$ non potrebbe essere un prodotto di primi, in contrasto col teorema fondamentale.

**9.5.** Assegnato l'intero positivo $n$, quanti tra i numeri $1,2,\ldots,n$ sono primi con $n$? Qual è, cioè, il numero $\varphi(n)$ degli $x\in\mathbf{N}$ tali che $1\leqslant x\leqslant n$, $(x,n)=1$? La funzione $\varphi$: $\mathbf{N}\to\mathbf{N}$ così definita si chiama *funzione* $\varphi$ *(ovvero indicatore) di Eulero*. Ad esempio, $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, ecc. In qualche caso il calcolo di $\varphi(n)$ è semplice. Ad esempio, se $p$ è primo, allora $\varphi(p)=p-1$; si vede anche subito che $\varphi(p^n)=p^n-p^{n-1}$: ciò si ottiene osservando che non sono primi con $p^n$ i soli multipli di $p$: $p,2p,\ldots,p^n-p,p^n$. Per calcolare $\varphi(n)$ nel caso generale basta provare (e lo faremo nel paragrafo 11.12.) che $\varphi(r\cdot s)=\varphi(r)\cdot\varphi(s)$ se $(r,s)=1$. Allora se $n=p_1^{n_1}\cdots p_r^{n_r}$ ($p_i$ primi distinti) si calcola subito:

$$\varphi(n)=(p_1^{n_1}-p_1^{n_1-1})\,(p_2^{n_2}-p_2^{n_2-1})\cdots(p_r^{n_r}-p_r^{n_r-1}).$$

Ad esempio, $\varphi(72)=\varphi(2^3\cdot 3^2)=\varphi(2^3)\,\varphi(3^2)=(2^3-2^2)\,(3^2-3)=24$.

**Esercizi**

1) Si verifichi la regola data in 9.3. per il calcolo del M.C.D. e m.c.m. di due numeri, partendo dalla fattorizzazione in primi.
2) Si estenda la regola di cui sopra al caso di $n(>2)$ numeri.
3) Se $a=p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$ (primi distinti), quanti sono i divisori di $a$?