ALCUNE APPLICAZIONI DELLA SECONDA FORMA DEL PRINCIPIO DI INDUZIONE

Le dimostrazioni dei seguenti notevoli teoremi sono applicazioni della seconda forma del Principio di Induzione:

Teorema Fondamentale dell' Aritmetica in $\mathbb{N}$

Sia $n \in \mathbb{N}$, $n \geq 2$. Allora:
i) n o è primo o è prodotto di numeri primi;
ii) se $n = p_1 p_2 \ldots p_t = q_1 q_2 \ldots q_s$ (con p_i, q_j numeri primi), allora $t = s$ ed è possibile riordinare i fattori q_i in modo che sia $p_i = q_i$ per ogni $i = 1,\ldots,t$.

Dim. *i)* La dimostrazione procede per induzione su n. Si utilizzerà la seconda forma del Principio d'Induzione.
Se $n = 2$, n è primo e dunque la *i)* è vera. Pertanto la base d'induzione è verificata. Sia allora $n > 2$ e si supponga la *i)* vera per ogni numero intero t tale che $2 \leq t < n$. Si possono distinguere due casi.

I) n è privo di divisori non banali. Allora n è un intero primo e la *i*) è verificata.

II) n possiede divisori non banali. Siano dunque n_1 ed n_2 divisori non banali di n tali che $n = n_1 n_2$, con $2 \leq n_1, n_2 < n$. Applicando l'ipotesi d'induzione si ha che sia per n_1 che per n_2 la *i)* è vera, per cui esisteranno numeri primi p_i e q_j tali che

$$n_1 = p_1 \ldots p_r \, , \, n_2 = q_1 \ldots q_l .$$

Allora

$$n = p_1 \ldots p_r \, q_1 \ldots q_l$$

e l'asserto è dimostrato.

ii) La dimostrazione si omette.

Algoritmo della divisione euclidea in $\mathbb{N}$

Siano $m,n \in \mathbb{N}$, $n \neq 0$. Allora esistono e sono univocamente determinati $q,r \in \mathbb{N}$ (detti rispettivamente quoziente e resto della divisione di m per n) tali che

$$m = nq + r \quad con \; 0 \leq r < n.$$

Dim. (Esistenza) Si ragionerà per induzione su m, applicando il Principio nella seconda forma.
Sia $m = 0$. Allora $0 = n \cdot 0 + 0$ e basta porre $q = 0 = r$.
Sia allora $m > 0$ e si supponga l'asserto vero per ogni numero naturale t tale che $0 \leq t < m$..
Se $m < n$, essendo $m = n \cdot 0 + m$, basta porre $q = 0$, $r = m$.
Se $m \geq n$, sarà $0 \leq m - n < m$, e, per ipotesi d'induzione, esistono q_1 ed r_1 tali che
$m - n = nq_1 + r_1$ con $0 \leq r_1 < n$.
Allora
$m = n + n\,q_1 + r_1 = n(1 + q_1) + r_1$
per cui, posto $q = 1 + q_1$ e $r = r_1$, si ha $m = nq + r$ con $0 \leq r < n$, come richiesto.
La dimostrazione dell'unicità di quoziente e resto viene omessa.