Seconda formulazione del Teorema Cinese del Resto - versione generale

Siano $n_1, \ldots, n_s$ interi positivi a due a due coprimi. Allora la seguente applicazione è un isomorfismo di anelli:

$$\varphi : \mathbb{Z}_{n_1 \cdots n_s} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

$$[a]_{n_1 \cdots n_s} \mapsto ([a]_{n_1}, \ldots, [a]_{n_s}) \qquad \text{per ogni } a \in \mathbb{Z}$$

<u>Dimostrazione (in breve)</u>: La buona definizione è conseguenza della transitività della relazione di divisibilità. La proprietà di omomorfismo di anelli è di facile verifica. L'iniettività, infine, è garantita dall'ipotesi di coprimalità. Infatti, in generale, per ogni $a \in \mathbb{Z}$, vale l'implicazione:

$$n_i | a \text{ per ogni } i \in \{1, \ldots, s\} \implies \text{mcm}(n_1, \ldots, n_s) | a$$

e, nel caso presente, **essendo i numeri n_1,..., n_s a due a due coprimi**, vale l'identità

$$\text{mcm}(n_1, \ldots, n_s) = n_1 \cdots n_s$$

Ciò prova che il nucleo di φ è ridotto al solo zero.
Poiché gli insiemi di partenza e di arrivo sono entrambi finiti e della stessa cardinalità, l'iniettività equivale alla bigettività. □

<u>Osservazione</u>: Nelle ipotesi suindicate, la suriettività dell'applicazione φ equivale alla risolubilità del sistema di congruenze lineari:

$$\begin{array}{cccc} x & \equiv & b_1 & \text{mod}(n_1) \\ \vdots & & \vdots & \vdots \\ x & \equiv & b_s & \text{mod}(n_s) \end{array}$$