Proposizione. *Sia R un anello commutativo finito di cardinalità $n \geq 2$. Se n è senza fattori quadrati, allora R è isomorfo a $\mathbf{Z}_n$.*

Dimostrazione. Per induzione. Se $n = p$ è un primo, allora il teorema di Lagrange implica che l'ordine dell'elemento 1 nel gruppo additivo di R divide p. Poiché $1 \neq 0$, l'ordine di 1 è per forza *uguale* a p. Questo implica che R consiste in multipli di 1. L'applicazione $\mathbf{Z}_p \longrightarrow R$ che manda $\overline{a}$ in $1 + 1 + \ldots + 1$ (a volte) è quindi un isomorfismo.

Se n non è primo, scriviamo m per l'ordine dell'elemento 1 nel gruppo additivo di R. Se $m = p$ è primo, allora R è uno spazio vettoriale sul campo $\mathbf{Z}_p$ con moltiplicazione data da

$$\overline{a}x = \underbrace{x + x + \ldots + x}_{a \text{ volte}}, \qquad (\overline{a} \in \mathbf{Z}_p \text{ e } x \in R.)$$

Come ogni spazio vettoriale R ammette una base su $\mathbf{Z}_p$ e quindi $n = \#R$ è una potenza di p. Poiché n è senza fattori quadrati si ha che $n = p$. Contraddizione.

Quindi m non è primo. Scriviamo $m = a \cdot b$ per certi interi $a, b > 1$. Sia $I = (a)$ l'ideale di R generato da $a = 1+1+\ldots+1$ (a volte) e sia $I = (b)$ l'ideale di R generato da $b = 1+1+\ldots+1$ (b volte). Si ha che $IJ = (m) = \{0\}$. Per il Teorema di Lagrange $ab = m$ divide n. Poiché n è senza fattori quadrati, a e b sono quindi coprimi. Per il Teorema di Bézout si ha quindi che $I + J = R$.

Possiamo adesso applicare il Teorema cinese del resto e troviamo un isomorfismo di anelli

$$R \;\cong\; R/IJ \;\cong R/I \times R/J.$$

Poiché m è l'ordine di 1 nel gruppo additivo di R, si ha che $a \neq 0$ e $b \neq 0$ in R. Questo implica che $I \neq \{0\}$ e $J \neq \{0\}$ e che gli anelli R/I e R/J hanno quindi *meno* di $n = \#R$ elementi. *Per induzione* ci sono quindi isomorfismi $R/I \cong \mathbf{Z}_u$ e $R/J \cong \mathbf{Z}_v$ per certi interi $u = \#(R/I)$ e $v = \#(R/J)$.

Poiché n è uguale a uv e n non ha fattori quadrati, u e v sono coprimi. Per il Teorema cinese del resto si ha quindi che

$$R \;\cong\; \mathbf{Z}_u \times \mathbf{Z}_v \;\cong\; \mathbf{Z}_{uv} \;=\; \mathbf{Z}_n$$

come richiesto.