Invertibilità di classi di resto rispetto al prodotto

Leonardo Bizzoni

October 19, 2023

Un elemento $[a]_n \in \mathbb{Z}_n$ si dice **invertibile** rispetto al prodotto se $\exists\ [b]_n \in \mathbb{Z}_n \mid [a]_n[b]_n = [1]_n$

Un criterio per decidere quando un elemento di $\mathbb{Z}_n$ è invertibile è il seguente:

> Siano $n \in \mathbb{Z} > 1,\ a \in \mathbb{Z}$. La classe di resto $[a]_n$ è invertibile in $\mathbb{Z}_n$ sse a, n sono coprimi.

Inoltre se $[a]_n$ è invertibile allora il suo **inverso** $([a]_n)^{-1}$ è **unico**.

1 Esempio

$[3]_6[b]_7$ non è invertibile in quanto $\text{MCD}(3, 6) = 3$.
$[3]_7[b]_7$ è invertibile in quanto $\text{MCD}(3, 7) = 1$ e $b = 5$ è la soluzione.