Calcolo dell'inverso moltiplicativo modulare

Determiniamo l'inverso $[x]$ di $[a] \in \mathbb{Z}/n\mathbb{Z}^*$.

Algoritmo di Euclide esteso

$$ax \equiv 1 \mod n \iff ax + ny = 1;$$

visto che $(a, n) = 1$, l'algoritmo di Euclide esteso permette di trovare x.

ϕ di Eulero

$$a^{-1} \equiv a^{\phi(n)-1} \mod n$$

veloce se si conosce la fattorizzazione di n con quadrature successive.