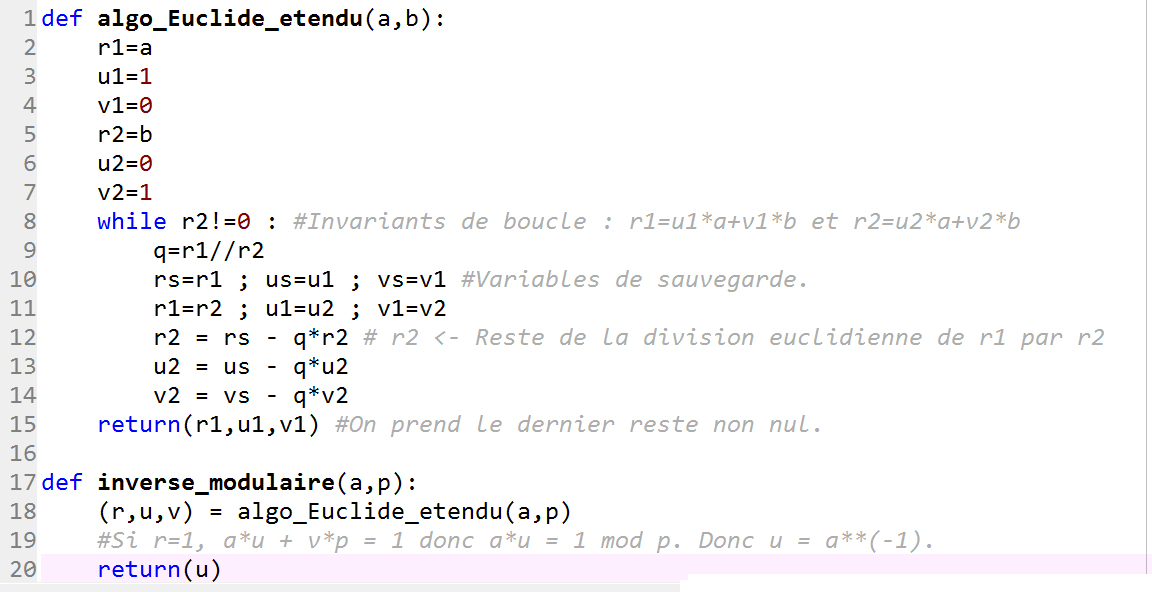
**Annexes**

Algorithme d’exponentiation rapide :


\mbox{puissance}(x,\,n)=\left\{
\begin{matrix} x, & \mbox{si }n\mbox{ = 1} \\ 
\mbox{puissance}(x^2,\,n/2), & \mbox{si }n\mbox{ est pair} \\
x\times\mbox{puissance}(x^2,\,(n-1)/2), & \mbox{si }n >\mbox{2 est impair} \\
\end{matrix}\right.


(Source : <http://fr.wikipedia.org/wiki/Exponentiation_rapide>)

Algorithme d’Euclide étendu et inverse modulaire :



Complexité de l’algorithme d’Euclide étendu : .