Exercice 1 :

1) Donner le programme qui implémente l'algorithme naïf de teste de primalité (TD2 exo2)
2) Donner le programme qui calcule le plus grand diviseur commun gcd
3) Donner le programme qui calcule Z_n^* où $\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n-1 \text{ and } \gcd(a,n) = 1\}$.

4) Donner le programme qui calcule les racines primitives sous modulo n
5) Donner le programme qui calcule les facteurs premiers avec leurs puissances pour un nombre *n*

Exercice 2 : (devoir à domicile)

Basant sur la solution du partie 4 de l'Exercice N°5 dans le TD3 et celle de l'exercice 1 de ce TP.

6) Donner le programme qui implémente le certificat pour un nombre premier n avec les trois conditions de primalité.

7) Implémenter l'algorithme de vérification de primalité (Prime certificate checking) du TD 3