Laboratoire 15

- **Buts**
  - Implantation de fonctions simples
- **Travail à réaliser**
  - Implanter une fonction qui retourne le plus grand diviseur commun entre deux nombres entiers passés en paramètre. Utiliser l'algorithme d'Euclide `https://fr.wikipedia.org/wiki/Algorithme_d%27Euclide` pour réaliser cette implantation.
  - Implanter la fonction d'exponentiation modulaire $b^e \mod m$, où b, e et m sont des entiers positifs. Pour implanter cette fonction efficacement, on peut remarquer que si e est pair, sa valeur vaut $((b^2) \mod m)^{(e/2)}$, ce qui permet de diviser par 2 le nombre de multiplications. Si b est impair, sa valeur vaut : $b \cdot b^{e-1} \mod m$. On en dérive l'algorithme efficace donné ci-dessous, à implanter sous la forme d'une fonction.
- **Délai**
  - Fin de la séance

Exponentiation modulaire

Input: $b, e, m \in \mathbb{N}$
Result: $r = b^e \mod m$

```
1 r ← 1
2 while e > 0 do
3 |   if e mod 2 = 0 then
4 |   |   b ← b² mod m; e ← e/2
5 |   else
6 |   |   r ← r · b mod m; e ← e − 1
7 end
```