TD Maple n°6. RSA.

Exercice 1 *Cryptage*

1. Construire une procédure `RSA` qui prend pour arguments deux nombres premiers p et q, qui propose une clé publique (n, e) associée et qui donne également la clé privée $(\varphi(n), d)$ correspondante. (On pourra créer l'entier e de façon aléatoire avec la commande `rand`).
2. Tester cette procédure avec de grands nombres premiers. (On pourra générer de grands nombres premiers à l'aide de la commande `ithprime`).

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

Exercice 2 *Piratage*

Bob et ses amis ne semblent pas avoir compris l'importance de prendre de grands nombres pour construire un code RSA. Ils ont publié les clés (n, e) suivantes, et les ont utilisé pour échanger les messages cryptés C suivants. Déterminer dans chaque cas la clé secrète $(\varphi(n), d)$ et retrouver les messages originaux. (On pourra faire le premier cas à la main...).

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.
3. $n = 667$, $e = 493$, $C = 10$.
4. $n = 1763$, $e = 611$, $C = 2$.
5. $n = 3599$, $e = 31$, $C = 60$.

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

Exercice 3 *Densités*

1. On a déjà vu qu'il existait une infinité de nombres premiers. Si l'on veut être plus précis, on peut se demander quelle est la propostion de nombres premier parmi l'ensemble des nombres entiers. Por cela, on commence par calculer la densité de nombres premiers dans l'ensemble $\{1, \ldots, n\}$ (i.e. le nombre de nombres premiers présents dans $\{1, \ldots, n\}$ divisé par le nombre d'entiers) puis faire tendre n vers l'infini.
   (a) Construire une procédure d'argument n qui renvoie la densité de nombres premiers dans $\{1, \ldots, n\}$. (Pour gagner un peu de temps, on pourra parcourirs les nombres impairs entre 3 et n).
   (b) Calculer cette densité pour $n = 10,\ 100,\ 1\,000,\ 10\,000,\ 1\,000\,000$.
2. On appelle nombres premiers jumeaux tous couples d'entiers $(p, p+2)$ tels que p et $p+2$ sont tous deux premiers.
   (a) Écrire une procédure d'argument n qui renvoie la densité de nombres premiers jumeaux présents dans $\{1, \ldots, n\}$.
   (b) Étudier cette densité quand n grandit.

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆