Feuille de TP n°1

Exercice 1. 1. Programmer le calcul du symbole de Jacobi de deux entiers. On pourra vérifier le résultat en utilisant la fonction Maple `numtheory[jacobi]`.

2. Implémenter l'algorithme de Solovay–Strassen.

***

Exercice 2. L'algorithme de Miller-Rabin repose sur la proposition suivante :

Proposition. *Soit p un nombre premier impair et soit a un nombre entier premier avec p. On écrit $p-1=2^r m$, avec m impair. Alors l'une des conditions suivantes est vérifiée : $a^m \equiv 1 \pmod{p}$ ou pour un $s \in \{0,\dots,r-1\}$, $a^{2^s m} \equiv -1 \pmod{p}$.*

On en déduit un test de non-primalité. Si n est un entier, $n-1=2^r m$ avec m impair, et s'il existe un $a \in \{1,\dots,n-1\}$ tel que $a^m \not\equiv 1 \pmod{n}$ et pour tout $s \in \{0,\dots,r-1\}$, $a^{2^s m} \not\equiv -1 \pmod{n}$, nécessairement, n est composé. Dans ce cas, on dit que a est un *témoin de non-primalité de Miller-Rabin de n.*

En outre, on peut montrer que si n est composé, au moins $3/4$ des entiers de $\{1,\dots,n-1\}$ sont des témoins de non-primalité de Miller-Rabin de n. On peut donc effectuer un test probabiliste de primalité efficace : en tirant suffisamment de nombres entiers a au hasard, si les conditions de la proposition ci-dessus sont toujours vérifiées, alors n est *probablement premier.*

1. Implémenter l'algorithme de Miller-Rabin.

2. Démontrer la proposition. On pourra utiliser le petit théorème de Fermat.