Exercice I: Rabin-Miller

Le test primalité de Rabin-Miller pour un entier n : S'il existe a et $i \geq 1$ tels que 2^i divise $n-1$ et que l'on ait $a^{\frac{n-1}{2^{i-1}}} = 1[n]$ avec $a^{\frac{n-1}{2^i}} \neq \pm 1[n]$, alors n n'est pas premier.

1) Quelle fonction utiliser pour une puissance rapide modulaire ? Etudiez par cette méthode la valeur de retour de $(-1)^{101}[7]$ et de $(-1)^{101}[p]$ où p est grand.

2) Créez d'abord une fonction `ramil1(n)` qui effectue ce test mais en utilisant pour l'instant qu'un seul témoin a. (On prendra par exemple $a = 2$). On évitera de devoir factoriser $n-1$.

3) Pour une valeur de n de votre choix (non première), donner toutes les valeurs de a pour lesquelles on n'a pas de réponse sure. Comparer ce nombre avec $phi(n)/4$.

4) Si la probalilité d'avoir un mauvais témoin est majorée par 1/4, combien de temoins faut il utiliser pour avoir une réponse sure a 99.9%

5) Programmez un test de rabin-miller avec cette fiabilité.

Exercice II:

finir TP13 sur log discret.

[1] http ://www.math.jussieu.fr/∼han/agreg