TD tests de primalité probabilistes

12 janvier 2024

1 Test de Fermat

Le petit théorème de Fermat assure que, si n est un nombre premier alors pour tout a premier avec n (donc en particulier pour tout $a \in \{1, \dots n-1\}$ on a : $a^{n-1} \equiv 1 \mod n$.

On dit qu'un entier n passe le test de Fermat pour un entier $a \in \{1, \dots n-1\}$ si $a^{n-1} \equiv 1 \mod n$.

1. Redémontrer le petit théorème de Fermat.
2. Ecrire une fonction `expo_modulaire` prenant en entrée trois entiers naturels `x,n,p` et calculant efficacement $x^n \mod p$. On justifiera que le nombre de produits modulaires effectués est en $O(\log n)$.
3. En exploitant le petit théorème de Fermat et en expliquant la démarche, concevoir un algorithme de type Monte Carlo à erreur unilatérale permettant de tester si un entier est premier. Ecrire une fonction `est_premier_fermat` implémentant cet algorithme qu'est le test de primalité de Fermat.

   La réciproque du petit théorème de Fermat est fausse : il existe des entiers composés n tels que pour tout a premier avec n, $a^{n-1} \equiv 1 \mod n$: on les appelle les nombres de Carmichael. Ainsi, le test de primalité de Fermat ne permet pas de distinguer les nombres premiers et les nombres de Carmichael.
4. Montrer que, si n n'est pas un nombre de Carmichael, alors la probabilité de faux positif sur n avec `est_premier_fermat` est inférieure ou égale à 1/2. (Indication : Observer que $\{a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \mod n\}$ est un sous groupe de $(\mathbb{Z}/_{n\mathbb{Z}})$).
5. En ignorant l'influence des nombres de Carmichael, écrire une fonction `est_presque_premier_fermat` résolvant `PREMIER` et dont la probabilité de renvoyer oui alors que son entrée est composée est inférieure à 10^{-20}. Justifier la démarche.

2 Test de Miller Rabin

Une variante du test de primalité de Fermat implémenté ci-dessus est le test de primalité de Miller-Rabin.

Ce dernier repose sur le résultat R suivant :

Si n est un nombre premier impair tel que $n-1 = 2^s \times m$ avec m impair alors pour tout $a \in \{1, \dots, n-1\}$ l'une des deux conditions suivantes est vérifiée :

(1) $a^m \equiv 1 \mod n$
(2) $\exists d \in \{0, \dots, s-1\}$ tel que $a^{2^d \times m} \equiv -1 \mod n$

1. Supposons que n est un nombre premier. Donner les racines carrées de 1 dans $\mathbb{Z}/_{n\mathbb{Z}}$.
2. En déduire le résultat R.

   Un élément $a \in \{1, \dots, n-1\}$ tel que ni (1) ni (2) ne soit vraie s'appelle un témoin de Miller-Rabin pour n.
   Un élément $a \in \{1, \dots, n-1\}$ tel que (1) ou (2) soit vraie s'appelle un co-témoin de Miller-Rabin pour n.
   On va montrer que si n est un entier impair composé et que l'on choisit a au hasard dans $\mathbb{Z}/_{n\mathbb{Z}}$, alors on a au moins une chance sur deux que n ne passe pas le test de Fermat pour a ou que a soit un témoin de Miller Rabin pour n.

3. Premier cas : $n = q^e$ avec q premier et $e \in \mathbb{N}^*, e \neq 1$. On pose $t = 1 + q^{e-1}$
   (a) Montrer que $t^n \equiv 1 \mod n$.
   (b) En déduire que n ne passe pas le test de Fermat avec t.
   (c) Montrer que dans ce cas, pour chaque d tel que n passe le test de Fermat avec d alors n ne passe plus le test de Fermat avec dt et que les dt sont distincts modulo n.
   (d) Conclure.

4. Montrer que pour un nombre impair composé n, il y a au moins un co-témoin de Miller Rabin qui satisfait (1) et un co-témoin de Miller Rabin qui satisfait (2).

5. Si on n'est pas dans le premier cas, justifier que n est factorisable en $q \times r$ avec q et r premiers entre-eux et différents de 1.
6. Deuxième cas : $n = qr$. On va montrer qu'il y au moins autant de témoins de Miller Rabin pour n que de co-témoins de Miller Rabin. On considère h le co-témoin de Miller Rabin de n qui satisfait la propriété (2) avec la valeur de d maximale.
   (a) Justifier l'existence de $t \in \mathbb{Z}/_{n\mathbb{Z}}$ tel que $t \equiv h \mod q$ et $t \equiv 1 \mod r$.
   (b) Montrer que $t^{2^d \times m} \equiv -1 \mod q$ et $t^{2^d \times m} \equiv 1 \mod r$.
   (c) En déduire que t est un témoin de Miller Rabin pour n. Fixons cette valeur de t.
   (d) Montrer que pour chaque co-témoin de Miller Rabin d de n, on obtient un témoin de Miller Rabin différent par la valeur $dt \mod n$.
   (e) Conclure
7. Concevoir un algorithme Monte Carlo à erreur unilatérale déterminant si un entier n est premier avec une bonne probabilité. Justifier votre construction et indiquer la probabilité de faux positif.