UNIVERSITÉ DE RENNES 1

Préparation à l'agrégation

Tests de Solovay-Strassen et de Rabin-Miller

Dans les exercices suivants, N est un entier impair supérieur ou égal à 3 et a est un entier premier à N.

Test de Solovay-Strassen

Définition 1. *On dit que N vérifie la condition de Solovay-Strassen en base a si :*

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod{N}.$$

(Ici, $\left(\frac{a}{N}\right)$ désigne le symbole de Jacobi).
Si N vérifie la condition de Solovay-Strassen en base a et n'est pas premier, on dit que c'est un pseudo-premier de Solovay-Strassen (ou pseudo-premier d'Euler-Jacobi) en base a.

Exercice 1

1. Montrer que les nombres premiers impairs vérifient la condition de Solovay-Strassen en n'importe quelle base.
2. Montrer que si N vérifie la condition de Solovay-Strassen en base a, alors $a^{N-1} \equiv 1 \pmod{N}$.

Exercice 2

Le but de cet exercice est de montrer que si N n'est pas premier, alors pour au moins la moitié des éléments a de $\{2, ..., N-1\}$, N n'est pas pseudo-premier d'Euler-Jacobi en base a. (On notera que si a n'est pas premier à N, alors un simple calcul de pgcd permet de montrer que N n'est pas premier).

1. Montrer que la condition de Solovay-Strassen ne dépend que de la classe modulo N de a, et non de l'entier a lui-même.
2. Montrer que l'ensemble des $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ tels que N vérifie la condition de Solovay-Strassen en base a est un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^\times$.
3. En déduire que s'il existe un $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ tel que N ne vérifie pas la condition de Solovay-Strassen en base a, alors pour au moins la moitié des éléments a de $\{2, ..., N-1\}$, N n'est pas pseudo-premier en base a.
4. S'il existe un nombre premier p tel que $p^2 \mid N$, montrer que $1 + \frac{N}{p}$ est d'ordre p dans $(\mathbb{Z}/N\mathbb{Z})^\times$.
5. Sous la même condition, en déduire que pour $a = 1 + \frac{N}{p}$, on ne peut pas avoir $a^{N-1} \equiv 1 \pmod{p}$.

6. Toujours sous la même condition, en déduire qu'il existe un $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ tel que N ne vérifie pas la condition de Solovay-Strassen en base a.
7. On suppose maintenant que N est sans facteur carré, non premier. Soit p un diviseur premier de N. Montrer qu'il existe un entier a premier à N, tel que $a \equiv 1 \pmod{\frac{N}{p}}$ et $\left(\frac{a}{p}\right) = -1$.
8. Montrer qu'on a alors $\left(\frac{a}{N}\right) = -1$.
9. En déduire que N ne vérifie pas la condition de Solovay-Strassen en base a.

Test de Rabin-Miller

Définition 2. *Soient e, m les entiers tels que $N-1 = 2^e m$ avec m impair. On dit que N vérifie la condition de Miller-Rabin en base a si :*

- *ou bien $a^m \equiv 1 \pmod{N}$*
- *ou bien il existe un entier $0 \leqslant f < e$ tel que $a^{2^f m} \equiv -1 \pmod{N}$.*

Si N vérifie la condition de Miller-Rabin en base a et n'est pas premier, on dit que c'est un pseudo-premier de Miller-Rabin (aussi appelé pseudo-premier fort) en base a.

Exercice 3

Le but de cet exercice est de montrer quelques résultats utiles sur les carrés dans $\mathbb{Z}/n\mathbb{Z}$. Il n'est pas nécessaire de traiter l'exercice en entier pour faire les exercices suivants.

1. Soit k un corps et soit $s \in k$. Montrer que l'équation $x^2 = s$ a au plus 2 solution dans k. Pour quelles valeurs de s a-t-elle une seule solution ? (Attention au cas où k est de caractéristique 2).
2. Soit $n \geqslant 2$ un entier, et soit x un entier tel que $x^2 \equiv 1 \pmod{n}$ et $x \not\equiv \pm 1 \pmod{n}$. Montrer que le PGCD de $x-1$ et n est un diviseur de n autre que 1 et n (et donc que n n'est pas premier).
3. Soit $n \geqslant 2$ un entier sans facteur carré et soit $s \in \mathbb{Z}/n\mathbb{Z}$. Combien l'équation $x^2 = s$ a-t-elle de solutions ? (Indication : factoriser n).
4. Soient p un nombre premier impair, $v > 0$ un entier, et $s \in \mathbb{Z}/p^v\mathbb{Z}$ tel que $\left(\frac{s}{p}\right) = 1$. Montrer que l'équation $x^2 = s$ a exactement 2 solutions dans $\mathbb{Z}/p^v\mathbb{Z}$. (Indication : procéder par récurrence sur v à l'aide du lemme de Hensel).
5. Soit $v \geqslant 3$ un entier, et soit $s \in \mathbb{Z}/2^v\mathbb{Z}$ tel que $s \equiv 1 \pmod{8}$. Montrer que l'équation $x^2 = s$ a exactement 4 solutions dans $\mathbb{Z}/2^v\mathbb{Z}$.
6. Soit $n \geqslant 2$ un entier et soit $s \in \mathbb{Z}/n\mathbb{Z}$. Combien l'équation $x^2 = s$ a-t-elle de solutions ?

Exercice 4

1. Montrer que les nombres premiers impairs vérifient la condition de Miller-Rabin en n'importe quelle base.
2. Montrer que si N vérifie la condition de Miller-Rabin en base a, alors $a^{N-1} \equiv 1 \pmod{N}$.
3. Montrer que l'algorithme suivant (en Python) correspond bien à la définition donnée ci-dessus :

```
def rabin_miller(a, N):
        e = 1
        while N & (1 << e) == 0:
                e += 1
        x = pow(a, N >> e, N)
        if x == 1 or N - x == 1:
                return True
        while e > 1:
                e -= 1
                x = (x * x) % N
                if x == 1:
                        return False
                if N - x == 1:
                        return True
        return False
```

Exercice 5

Le but de cet exercice est de montrer que la condition de Miller-Rabin implique la condition de Solovay-Strassen.

On pose $N - 1 = 2^e m$ avec m impair, comme dans la définition. On suppose que N vérifie la condition de Miller-Rabin en base a.

1. Si $a^m \equiv 1 \pmod{N}$, montrer que $\left(\frac{a}{N}\right) = 1$ (indication : m est impair). En déduire que la condition de Solovay-Strassen est vérifiée dans ce cas.
2. On suppose désormais qu'il existe un entier $0 \leqslant f < e$ tel que $a^{2^f m} \equiv -1 \pmod{N}$. Soit p un diviseur premier de N. Notons α_p l'ordre de a dans $\mathbb{F}_p^\times$. Montrer que $v_2(\alpha_p) = f + 1$ (où v_2 désigne la valuation 2-adique).
3. En déduire que $p \equiv 1 \pmod{2^{f+1}}$.
4. Montrer que
$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{si } v_2(p-1) > v_2(\alpha_p) \\ -1 & \text{si } v_2(p-1) = v_2(\alpha_p) \end{cases} \pmod{p}$$
5. En déduire que $\left(\frac{a}{p}\right) = 1$ si et seulement si $p \equiv 1 \pmod{2^{f+2}}$.
6. Notons G le groupe quotient $\frac{1+2^{f+1}\mathbb{Z}}{1+2^{f+2}\mathbb{Z}}$ (la loi de groupe étant donnée par la multiplication). Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
7. Montrer que $\left(\frac{a}{p}\right) = 1$ si et seulement si l'image de p dans G est l'élément neutre.

8. En déduire que $\left(\frac{a}{N}\right) = 1$ si et seulement si l'image de N dans G est l'élément neutre.
9. En déduire que
$$\left(\frac{a}{N}\right) = \begin{cases} 1 & \text{si } f < e-1 \\ -1 & \text{si } f = e-1. \end{cases}$$
10. En déduire que la condition de Solovay-Strassen est vérifiée.
11. Montrer que si N n'est pas premier, alors pour au moins la moitié des éléments a de $\{2, ..., N-1\}$, N n'est pas pseudo-premier de Rabin-Miller en base a.