SÉANCE 8. LE TEST DE PRIMALITÉ DE MILLER-RABIN

Il est théoriquement facile de déterminer si un nombre entier n est premier ou non : il suffit d'effectuer la division euclidienne de n par tous les entiers m tels que $2 \leqslant m \leqslant \sqrt{n}$; si tous les restes sont non nuls, alors n est premier ; sinon, on a déterminé un diviseur non trivial de n.

En pratique, il n'est pas possible d'effectuer tous les calculs nécessaires lorsque le nombre entier n est suffisamment grand. Nous allons étudier un test de (pseudo-)primalité *probabiliste* : cet algorithme ne prouve pas qu'un nombre est premier, mais il permet de l'affirmer avec une probabilité d'erreur aussi petite que l'on souhaite.

Exercice 1 (Test de Fermat) — Le petit théorème de Fermat affirme que, si p est un nombre premier, alors

$$a^{p-1} \equiv 1 \pmod{p}$$

pour tout nombre entier a premier à p (c'est-à-dire tel que $p \nmid a$).

Soit $n \geqslant 2$ un nombre entier. Pour que n soit premier, la condition :

$$\forall a \in \mathbf{N}^*, \ \left(\operatorname{pgcd}(a,n) = 1 \Longrightarrow a^{n-1} \equiv 1 \pmod{n}\right) \tag{1}$$

est donc *nécessaire*. Cette condition-elle suffisante ?

1. Définir une fonction `TestFermat(n)`, qui renvoie `Succès` si la condition (1) est vérifiée, `Échec` si elle ne l'est pas.
2. Écrire une fonction `PremierFermat(x)` qui renvoie la liste des entiers $n \leqslant x$ pour lesquels la condition (1) est vérifiée.
3. Comparer le résultat de la question précédente avec la liste des nombres premiers inférieurs à x (cf. TD2). Que peut-on en conclure ? Quels sont les cinq premiers nombres composés vérifiant la condition (1) ?

Exercice 2 (Test de Fermat probabiliste) — Dans l'exercice précédent, la fonction `TestFermat(n)` requiert le calcul de a^{n-1} pour *tout* $a \in \{1, \dots, n-1\}$ tel que $\operatorname{pgcd}(a,n) = 1$. Si l'algorithme d'exponentiation est très efficace, il est évidemment très (trop) long de l'effectuer $\varphi(n)$ fois lorsque n est un très grand nombre (pour mémoire, $\varphi(n) = n-1$ si n est premier).

Pour tout entier $n \geqslant 2$, posons

$$H_n = \left\{ x \in (\mathbf{Z}/n\mathbf{Z})^\times \mid x^{n-1} = 1 \right\}.$$

1. Vérifier que H_n est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^\times$. En déduire que, si n ne vérifie pas la condition (1) de l'exercice précédent, alors

$$\operatorname{Card} H_n \leqslant \frac{1}{2}\varphi(n).$$

2. Supposons que l'on tire au sort un nombre entier a dans $\{1, \dots, n-1\}$ selon la loi uniforme. Démontrer que la probabilité que $\overline{a}$ (la classe de a modulo n) appartienne à H_n est inférieure à $\frac{1}{2}$.

3. Écrire une fonction `TestFermatProba(n)` qui :
   (i) tire au sort un nombre a entre 1 et $n-1$;
   (ii) renvoie « Échec » si $\text{pgcd}(a,n) \neq 1$;
   (iii) calcule sinon $a^{n-1} \pmod n$ et renvoie « Échec » si le résultat est différent de 1, « Succès » sinon.
4. Quel est le résultat de `TestFermatProba(n)` si n vérifie la condition (1) ?
5. Supposons que n ne vérifie pas la condition (1) et effectuons $k \geqslant 1$ répétitions indépendantes de `TestFermatProba(n)`. Quelle est la probabilité d'obtenir à chaque fois « Succès » ?
6. Sur des exemples, comparer le temps de calcul des algorithmes `TestFermat(n)` et `TestFermatP(n)`.

Exercice 3 (Test de Miller-Rabin) — Comme on l'a vu à l'exercice 1, le test de Fermat ne suffit pas pour déterminer si un nombre n est premier ou composé. Le *test de Miller-Rabin* est un raffinement du test de Fermat qui permet de le faire.

1. Soit $p > 2$ un nombre premier.
   (i) Quelles sont les solutions de l'équation $x^2 = 1$ dans $\mathbf{Z}/p\mathbf{Z}$?
   (ii) Écrivons $p = 1 + 2^h m$ avec $2 \nmid m$. Démontrer que tout $x \in \mathbf{Z}/p\mathbf{Z}$ vérifie la condition suivante :
   $$x^m = 1 \text{ ou } \exists k \in \{0,\dots,h-1\},\ x^{2^k m} = -1. \tag{2}$$
   Observer que l'on a $x^{p-1} = x^{2^h m} = 1$ et utiliser (i).
2. Écrire une fonction `TestMillerRabin(n)` qui prend en entrée un entier n *impair* et :
   (i) détermine les entiers h et m tels que $n = 1 + 2^h m$ avec $2 \nmid m$;
   (ii) tire au sort un nombre a entre 1 et $n-1$;
   (iii) renvoie « Échec » si $\text{pgcd}(a,n) \neq 1$;
   (iv) calcule sinon la suite des $a^{2^k m} \pmod n$ pour $k \in \{0,\dots,h\}$;
   (v) renvoie « Succès » si la suite obtenue est de la forme
   $$(1,\dots,1) \text{ ou } (*,\dots,*,n-1,1,\dots,1),$$
   renvoie « Échec » sinon.

Le théorème de Rabin affirme que, si n n'est pas premier, alors il existe au plus $\frac{\varphi(n)}{4}$ entiers $a \in \{1,\dots,n-1\}$ tels que $\overline{a}$ vérifie la condition (2).

3. Que peut-on dire de n si la fonction `TestMillerRabin(n)` renvoie « Échec » ?
4. Majorer la probabilité de n ne soit pas premier mais que $k \geqslant 1$ répétitions indépendantes de `TestMillerRabin(n)` ne renvoient que des succès.
5. Posons $n = 100129 \cdot 200257$. En théorie, la fonction `TestMillerRabin(n)` doit renvoyer « Échec » au moins trois fois sur quatre. Essayer de vérifier cela empiriquement.
6. Écrire une fonction `CribleMR(N,k)` affichant tous les nombres entiers entre 2 et N passant avec succès k répétitions indépendantes du test de Miller-Rabin. Pour $k = 1,2,\dots,10$, comparer le résultat de `CribleMR(1000,k)` avec celui de la fonction `Crible(1000)` du TP2.

7. Écrire une fonction `PremierSuivant(m)` déterminant le plus petit nombre $p \geqslant m$ passant avec succès dix répétitions indépendantes du test de Miller-Rabin. La probabilité que ce nombre soit premier est supérieure à

$$1 - \left(\frac{1}{4}\right)^{10} \simeq 0,999999.$$

Les questions suivantes donnent une preuve partielle du théorème de Rabin. Plus précisément, nous allons prouver que si le nombre entier $n = 1 + 2^h m$ (avec $2 \nmid m$) est composé, alors il existe $x \in (\mathbf{Z}/n\mathbf{Z})^\times$ ne vérifiant pas la condition (2).

Supposons tout d'abord que n soit de la forme p^α avec p premier et $\alpha \geqslant 2$. Posons $x = \overline{1+p}$.

7. Calculer $(1+p)^{p^{\alpha-1}}$ modulo p^α. Quelle conséquence peut-on en tirer quant à l'ordre de x ?

8. En déduire que l'on a $x^{n-1} \neq 1$, et donc que x ne vérifie pas la condition (2).

Nous supposons maintenant que n s'écrit sous la forme $n = uv$, avec $u, v > 1$ deux nombres premiers entre eux. Rappelons (*théorème des restes chinois*) que l'application

$$\lambda : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/u\mathbf{Z} \times \mathbf{Z}/v\mathbf{Z}, \quad a \pmod n \mapsto (a \pmod u, a \pmod v)$$

induit alors un isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^\times \xrightarrow{\sim} (\mathbf{Z}/u\mathbf{Z})^\times \times (\mathbf{Z}/v\mathbf{Z})^\times .$$

9. Démontrer que l'application $p_m : x \mapsto x^m$ réalise une bijection de $(\mathbf{Z}/n\mathbf{Z})^\times$ sur lui-même.

10. Soit x l'unique élément de $(\mathbf{Z}/n\mathbf{Z})^\times$ tel que $x^m = y$, avec $\lambda(y) = (\overline{-1}, \overline{1})$. Vérifier que x ne satisfait pas la condition (2).

11. Définir une fonction `TémoinsMR(n)` renvoyant le nombre d'entiers a dans $\{1, \ldots, n-1\}$ ne vérifiant pas la condition (2).