

TD/TP PRIMALITÉ

Références

- Demazure, *Cours d'algèbre*.
- Shoup, *A Computational Introduction to Number Theory and Algebra*.

Exercice 1 — Exponentiation rapide —

Soient A un anneau, a un élément de A .

1. Montrer que l'algorithme suivant renvoie a^n :
 $(x, y, n) \leftarrow (a, 1, n)$;
Tant que $n \neq 1$ faire :
 Si n pair : $(x, y, n) \leftarrow (x^2, y, n/2)$;
 Si n impair : $(x, y, n) \leftarrow (x^2, xy, (n-1)/2)$;
Renvoyer xy .
2. Implémenter cet algorithme dans Sage.
3. Montrer que l'algorithme suivant renvoie a^n :
Calculer la décomposition de n en base 2 : $n = \sum_{i=0}^k n_i 2^i$;
 $x \leftarrow a$;
Pour $i = k-1$ à 0 faire :
 $x \leftarrow x^2$;
 Si $n_i = 1$: $x \leftarrow ax$;
Renvoyer x .
4. En utilisant la méthode `bits()` de Sage, implémenter cet algorithme.
5. Comparer les temps de calcul des deux algorithmes pour $A = \mathbb{Z}/N\mathbb{Z}$ puis $A = \mathbb{Z}$.

Exercice 2 — Le test de Fermat —

1. Soit $n = pq$ avec p, q des nombres premiers tels que $\text{pgcd}(p-1, q-1) = 2$. Montrer que $a = 2$ est un témoin de Fermat de la non-primauté de n .
2. Montrer avec le critère de Fermat et à l'aide de Sage que les nombres de Fermat $F_n = 2^{2^n} + 1$ sont composés pour tout $5 \leq n \leq 10$.
3. On décide d'utiliser le critère suivant pour vérifier la primalité : n est premier à 30, et $a^{n-1} = 1 \pmod n$ pour $a \in \{2, 3, 5\}$. Quelles sont les plus petites valeurs de n pour lesquelles ce critère est en défaut ?
4. Calculer le plus petit témoin de Fermat (s'il en existe) pour beaucoup de nombres composés pris au hasard. Qu'observe-t-on ? Que peut-on en déduire sur l'efficacité de ce test ?

Exercice 3 — Nombres de Carmichael —

Soit n un entier, on dit que n est *pseudo-premier en base a* si $a^{n-1} = 1 \pmod n$. On rappelle qu'un *nombre de Carmichael* un entier composé n qui est pseudo-premier en toute base a première à n .

1. Montrer que tout nombre de Carmichael est impair.
2. Montrer que n est de Carmichael si et seulement s'il est composé, sans facteur carré et si pour tout facteur premier p de n , on a $p-1 \mid n-1$ (critère de Korselt).
3. Déterminer la liste des nombres de Carmichael $< 10^4$.

Exercice 4 — Critère de Miller-Rabin —

Soit $n > 1$ un entier impair. Posons $n-1 = 2^s t$ avec t impair.

On rappelle le critère de Miller-Rabin : s'il existe un entier a avec $1 < a < n$ tel que $a^t \not\equiv 1 \pmod n$ et $a^{2^i t} \not\equiv -1 \pmod n$ pour tout $0 \leq i \leq s-1$, alors n est composé, et a est appelé *témoin de Miller* de la non-primalité de n .

1. Déterminer le nombre de témoins de Miller pour le nombre de Carmichael $n = 561$.
2. Déterminer le plus petit entier composé n tel que ni 2, ni 3, ni 5 ne sont témoins de Miller pour n .
3. Étudier la proportion de témoins de Miller pour des entiers n pris au hasard.
4. Calculer le coût de chaque instance du test de Miller-Rabin.

Exercice 5 — Critère de Solovay et Strassen —

On rappelle la définition du symbole de Legendre : pour $a \in \mathbb{Z}$ et p premier, on pose

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \pmod p, \\ 1 & \text{si } a \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^\times, \\ -1 & \text{sinon.} \end{cases}$$

1. Soit $a \in \mathbb{Z}$ et $p \geq 3$ premier. Montrer que $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$.

Soit $n \geq 3$ un entier impair. Notons $n = p_1 \cdots p_r$ où les p_i sont des nombres premiers non nécessairement distincts. Le symbole de Jacobi est défini par

$$\left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right).$$

On dit que n est *pseudo-premier d'Euler en base a* si $a^{(n-1)/2} = \left(\frac{a}{n}\right) \pmod n$. Si cette condition n'est pas vérifiée, alors n est composé, et a est appelé *témoin de Solovay*.

1. Montrer que tout témoin de Fermat est aussi un témoin de Solovay.
2. Montrer que n est premier si et seulement si n est pseudo-premier d'Euler en base a pour tout entier a premier à n .
3. Montrer que si n n'est pas premier, alors au moins la moitié des entiers a premiers avec n tels que $1 < a < n$, sont des témoins de Solovay.
4. En déduire un test de primalité probabiliste (le test de Solovay-Strassen).