

L3 Calcul Formel

Université de Lorraine

TP 3 : Tests de primalité

Clément Dell'Aiera

Quelques remarques :

- Le TP est à rendre par mail avant le mercredi 21 octobre. Votre fichier sage doit être nommé *TP3_Nom* où vous remplacerez Nom par votre nom de famille. Essayez de commenter votre code, vous ne le faites pas assez. Un code mal commenté est un code incompréhensible.
- Dans l'énoncé et dans tous les suivants, les verbes "démontrer", "montrer", etc. impliquent que l'on attend de vous une démonstration mathématique écrite, tandis que les instructions "implémenter une fonction", "écrire un programme", etc. signifient que vous devez utiliser Sage.

1 Calcul rapide de puissance

1. Implémenter une fonction qui à deux entiers a et m retourne a^m .
2. Voici un algorithme dit rapide pour élever un entier à un certaine puissance. Si on écrit m en base binaire, soit $m = \overline{m_k \dots m_1 m_0}^{(2)} = \sum_{j=0}^k m_j 2^j$, on peut se servir récursivement de l'identité

$$a^m = a^{m_0} (a^{m_1} (a^{m_2} \dots)^2)^2$$

pour diminuer les coûts de calculs. Implémenter une telle fonction qui utilise moins de $2E[\log m]$ multiplications, avec E la partie entière.

2 Tests de primalité

2.1 Premier algorithme naïf

Le premier test de primalité qui vient à l'esprit est de parcourir à l'aide d'une boucle tous les entiers de 2 à $n - 1$ et de vérifier si l'un deux divise n . Un instant de réflexion permet de comprendre que l'on peut se limiter aux nombres inférieurs à \sqrt{n} . Pourquoi ?

Implémenter une fonction qui effectue ce test.

2.2 Test de Fermat

Nous allons utiliser le petit théorème de Fermat, que voici.

Théorème 1. Soient p un nombre premier et a un entier. Alors $a^{p-1} \equiv 1 \pmod{p}$ pour a premier à p et $a^p \equiv a \pmod{p}$ pour tout entier a .

Si l'on parvient à trouver un entier $a \in \{1, 2, \dots, n-1\}$ tel que $a^{n-1} \not\equiv 1 \pmod{n}$ alors n n'est pas premier. Un tel a est appelé un témoin de Fermat.

1. Implémenter une fonction $Fermat(a, n)$ qui prend deux entiers a et n en entrée, et qui retourne *True* si a est un témoin de Fermat pour n , *False* sinon.
2. Implémenter une fonction qui prend en entrée deux entiers n et M , qui effectue au plus M fois le test $Fermat(a, n)$ sur un nombre a tiré au hasard entre 2 et $n-1$, et qui s'arrête dès que $Fermat(a, n)$ renvoie *True*. Cette fonction doit retourner une chaîne de caractère : "n n'est pas premier" si elle a trouvé un témoin de Fermat, et "n est probablement premier" sinon.

2.3 Deux tests probabilistes

Importer le package *random* grâce à la commande *import random*. Que retourne l'évaluation de *random.randint(a, b)*, où a et b sont deux entiers ?

2.3.1 Test de Miller

Théorème 2. Soit $p > 2$ un nombre premier, et s et t , t impair, tels que $p-1 = 2^s t$. Soit a un entier non divisible par p . Alors, ou bien $a^t \equiv 1 \pmod{p}$, ou bien il existe un entier j tel que $0 \leq j < s$ et $a^{2^j t} \equiv -1 \pmod{p}$.

De ce théorème, on déduit que si n est un entier impair, alors l'existence d'un entier a , $1 < a < n$, tel que

$$a^t \not\equiv 1 \pmod{n} \quad \text{et} \quad a^{2^j t} \not\equiv -1 \pmod{n}$$

pour $j = 0, \dots, s-1$ assure que n est composé. Un tel a est appelé témoin de Miller pour n . (La méthode de ce numéro a été proposée par Gary Miller)

1. Implémenter une fonction $Miller(a, n)$ qui prend deux entiers a et n en entrée, et qui retourne *True* si a est un témoin de Miller pour n , *False* sinon.
2. Implémenter une fonction qui prend en entrée deux entiers n et M , qui effectue au plus M fois le test $Miller(a, n)$ sur un nombre a tiré au hasard entre 2 et $n-1$, et qui s'arrête dès que $Miller(a, n)$ renvoie *True*. Cette fonction doit retourner une chaîne de caractère : "n n'est pas premier" si elle a trouvé un témoin de Miller, et "n est probablement premier" sinon.

2.3.2 Test de Solovay-Strassen

Soit n et m deux entiers. On dit que n est un résidu quadratique modulo m s'il existe un entier a tel que $n \equiv a^2 \pmod{m}$, i.e. si n est un carré dans l'anneau $\mathbb{Z}/m\mathbb{Z}$. Si p est premier, le symbole de Legendre $\left(\frac{a}{p}\right)$ est un nombre défini comme valant 0 si p divise a , 1 si p ne divise pas a et a est un résidu quadratique modulo p , -1 sinon. Une formule due à Euler permet de calculer le symbole de Legendre grâce à l'algorithme des puissances rapides du premier numéro.

Proposition 1 (Euler). Soit p premier impair. L'anneau $\mathbb{Z}/p\mathbb{Z}$ possède p éléments qui sont des carrés : 0 et $\frac{p-1}{2}$ éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$. De plus $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Si $n \geq 3$ est impair, on rappelle que $\left(\frac{a}{n}\right)$ est le symbole de Jacobi, défini comme suit. On décompose n en facteurs premiers $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, alors

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

Théorème 3 (Solovay-Strassen). Soit $n > 2$ un entier impair tel que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ pour tout entier a premier à n . Alors n est premier.

On peut en déduire que si n est premier, $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ pour tout entier a premier à n , et si $n > 2$ est composé, l'ensemble des a premiers à n tels que $0 < a < n$ et $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ a au plus $\frac{\varphi(n)}{2}$ éléments.

1. Implémenter une fonction qui calcule le symbole de Jacobi. (Difficile, même avec le théorème de réciprocité quadratique) Si vous n'y arrivez pas, vous pouvez utiliser la fonction `kroncker(a, n)` que Sage a déjà en mémoire, et qui calcule le symbole de Jacobi.
2. Comme dans les numéros précédents, implémenter une fonction qui teste si un nombre est un témoin de Solovay-Strassen pour n , et ensuite une autre fonction qui effectue ce test aléatoirement au plus M fois.

2.4 Exercices

2.4.1 Indicatrice d'Euler

On dit qu'une fonction $f : \mathbb{N} \rightarrow \mathbb{N}$ est multiplicative si, lorsque $\text{pgcd}(n, m) = 1$, alors $f(nm) = f(n)f(m)$. Attention ce n'est pas une définition standard : généralement multiplicatif signifie respecter la multiplication, et ce de façon inconditionnelle. Une fonction multiplicative est déterminée par ses valeurs sur les puissances de nombres premiers. On note $\varphi(n)$ l'indicatrice d'Euler, i.e. le nombre d'entiers $< n$ et premiers avec n .

1. Montrer que si f est multiplicative, alors

$$g(n) = \sum_{d|n} f(d)$$

l'est aussi.

2. Montrer que

$$n = \sum_{d|n} \varphi(d).$$

2.4.2

1. Démontrer le petit théorème de Fermat.
2. Coin de la culture : chercher le théorème de réciprocité quadratique si vous ne le connaissez pas.