Test de Solovay-Strassen

Perrine Jouteur

Ce développement est particulièrement utile pour les personnes en option C, puisqu'il concerne un algorithme au programme de la modélisation. Je l'ai mis dans les leçons 120, 121, 123 et 190. On peut en trouver une exposition plus complète dans le livre *Cours d'algèbre algorithmique* de Demazure ou en anglais dans *A course in computational algebraic number theory* de Cohen.

1 Contexte et prérequis

Définition 1.1 Symbole de Jacobi.

Proposition 1.1 Coût de calcul d'un symbole de Jacobi en fonction de la taille de n.

2 Le développement

Considérons un entier n impair et supérieur à 3.

Proposition 2.1
L'entier n est premier si et seulement si pour tout entier a premier avec n, on a

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} [n].$$

Démonstration
• Faisons le sens direct. Si n est premier, alors le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est de cardinal $n-1$. Par intégrité de $\mathbb{Z}/n\mathbb{Z}$, pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $a^{\frac{n-1}{2}} \equiv \pm 1$ modulo n.
Notons H l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ tels que $a^{\frac{n-1}{2}} \equiv 1$ modulo n. Il s'agit d'un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Comme $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique, il existe un élément d'ordre $n-1$ dedans et donc cet élément n'est pas dans H. Ainsi H est un sous-groupe strict, et il contient donc au plus $\frac{n-1}{2}$ éléments (il est au moins d'indice 2).
Maintenant si a est un carré modulo n, $a = b^2$, alors $a^{\frac{n-1}{2}} = b^{n-1} = 1$ modulo n par théorème de Lagrange. Donc H contient tous les carrés. Or il y a $\frac{n-1}{2}$ carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$, et donc H est exactement l'ensemble des carrés. Donc si a n'est pas un carré modulo n, alors a n'est pas dans H donc $a^{\frac{n-1}{2}} \equiv -1$ modulo n.

• Procédons au sens réciproque. Supposons donc que pour tout a tel que a est premier avec n, on ait $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ modulo n.

Étape 1 : montrons que n est sans facteur carré.
Supposons qu'il existe un nombre premier p tel que p^2 divise n, c'est-à-dire que $n = p^2 m$, avec $m \in \mathbb{N}^*$. Considérons l'entier $a := 1 + pm$. Remarquons que a est premier avec n, car on peut écrire la relation de Bézout suivante :

$$a(1 - pm) + mn = 1.$$

Donc par hypothèse, $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\ [n]$, et donc $a^{n-1} \equiv 1\ [n]$.
D'autre part, par binôme de Newton,

$$a^p = \sum_{k=0}^{p} \binom{p}{k} (pm)^k = 1 + p^2 m + \binom{p}{2} p^2 m^2 + \cdots + p^p m^p.$$

Ainsi $a^p \equiv 1\ [n]$. Donc l'ordre de a modulo n divise p, et comme p est premier il est en fait égal à p.
On a vu plus haut que $a^{n-1} \equiv 1\ [n]$ donc p divise $n-1$, ce qui est absurde, et donc n est sans facteur carré.

Étape 2 : montrons que n est premier. On écrit $n = p_1 \cdots p_r$ avec les p_i des nombres premiers distincts. Supposons que r soit supérieur à 2.
On peut alors choisir $\alpha_1, \cdots, \alpha_{r-1}, \alpha_r$ des entiers tels que $\alpha_1 = 1$, $\alpha_i \in [\![1, p_i - 1]\!]$, et pour tout $i = 2, \cdots, r-1$,

$$\left(\frac{\alpha_i}{p_i}\right) = 1 \text{ et } \left(\frac{\alpha_r}{p_r}\right) = -1.$$

Par théorème chinois, il existe un unique entier a entre 1 et $n-1$ tel que $a \equiv \alpha_i \ [p_i]$ pour tout i. Cet entier a est premier avec chacun des p_i donc est premier avec n. L'hypothèse s'applique donc pour a :

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ [n].$$

En particulier, $\left(\frac{a}{n}\right) \equiv \alpha_1^{\frac{n-1}{2}} \ [p_1]$. Or on a choisi $\alpha_1 = 1$ donc $\left(\frac{a}{n}\right) \equiv 1 \ [p_1]$.
D'un autre côté, $\left(\frac{a}{n}\right) = \left(\frac{\alpha_1}{p_1}\right) \cdots \left(\frac{\alpha_{r-1}}{p_{r-1}}\right) \left(\frac{\alpha_r}{p_r}\right) = -1$.
Ceci est absurde, donc $r = 1$ et n est premier. ■

Proposition 2.2 Si n est composé, il y a au plus $\phi(n)/2$ entiers a entre 1 et $n-1$ vérifiant

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} [n] \quad (*).$$

Démonstration
Supposons que n soit composé.
Remarquons d'abord que si a est un entier entre 1 et $n-1$ qui vérifie $(*)$, alors a est premier avec n, puisque l'égalité $(*)$ assure que le symbole de Jacobi $\left(\frac{a}{n}\right)$ est non nul.
Ensuite, l'ensemble des entiers a premiers avec n qui vérifient $(*)$ forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. En effet, il contient $\overline{1}$, et si a_1, a_2 conviennent alors par multiplicativité du symbole de Jacobi,

$$\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) \equiv a_1^{\frac{n-1}{2}} a_2^{\frac{n-1}{2}} \equiv (a_1 a_2)^{\frac{n-1}{2}} \ [n].$$

et $\left(\frac{a_1^{-1}}{n}\right) = \left(\frac{a_1}{n}\right) \equiv a_1^{\frac{n-1}{2}} \equiv (a_1^{-1})^{\frac{n-1}{2}} \ [n]$.

Comme on a supposé que n est composé, ce sous-groupe est strict d'après la proposition précédente. Et ainsi il est au moins d'indice 2, donc de cardinal au plus $\phi(n)/2$. ■

Définition 2.1 Le test de Solovay-Strassen consiste à choisir au hasard un entier a entre 1 et $n-1$, et à faire le calcul du symbole $\left(\frac{a}{n}\right)$.
• Si on trouve 0, c'est que a n'est pas premier avec n et donc qu'on a trouvé un facteur de n.
Sinon, on le compare à $a^{\frac{n-1}{2}}$. Si c'est différent, alors n est composé. Si c'est égal, on recommence avec un autre entier a.

Définition 2.2 On appelle témoin de Solovay Strassen un entier a entre 1 et $n-1$ qui ne vérifie pas $(*)$.

Proposition 2.3 Si n est composé, la probabilité qu'il faille N tests pour trouver un témoin de Solovay-Strassen est de $1/2^N$.

Démonstration
On suppose qu'on effectue les tirages au sort de manière uniforme entre 1 et $n-1$, à chaque test, c'est-à-dire que si on pioche un entier qui n'est pas un témoin, on retire ensuite sans écarter la possibilité de retirer ce même entier.
La probabilité qu'il faille N tirages exactement pour trouver un témoin de Solovay Strassen est égale à la probabilité que les $N-1$ premiers tirages ne donnent pas de témoin et que le Nième en donne un. Comme les tirages sont indépendants, c'est égal à

$$(\text{proba de ne pas trouver de témoin})^{N-1} \times (\text{proba de trouver un témoin}).$$

Or d'après la proposition précédente, la probabilité de tirer un témoin de Solovay Strassen en un tirage est de $1/2$. D'où le résultat. ■