Tests de primalité

⟶ Réfs : Perrin p74-75 ("⇐" prop 2), Demazure (tout le reste)

Rappel : Théorème de Fermat : Soit p un nombre premier. Alors pour tout entier a premier à p, $a^{p-1} \equiv 1 [p]$ (et pour tout entier a, $a^p \equiv a [p]$)

Si le théorème était une équivalence, on pourrait créer un test de primalité à partir de cela. Cependant, la réciproque est fausse...

Définition : Un entier $n \geq 2$ est appelé nombre de Carmichael si n n'est pas premier (on dit aussi que n est composé) et si pour tout entier a premier à n, $a^{n-1} \equiv 1 [n]$ ($\Leftrightarrow$ n est composé et pour tout entier a, $a^n \equiv a [n]$)

Proposition 1 (Critère de Korselt) Soit $n \geq 2$ un entier. Alors n est de Carmichael si et seulement si n est sans facteur carré, et pour tout facteur premier p de n, $p-1$ divise $n-1$.

Ce critère nous sera utile pour la suite.

Puisque le test qui découle du théorème de Fermat n'est pas satisfaisant, nous allons essayer d'obtenir une CNS qui permet de se débarasser des nombres de Carmichael.

Proposition 2 : Soit n un entier impair, supérieur ou égal à 3. Alors n est premier si et seulement si pour tout entier a premier avec n, on a $\underbrace{\left(\frac{a}{n}\right)}_{\text{symbole de Jacobi !}} \equiv a^{\frac{n-1}{2}} [n]$

On pourra alors, à partir de cela, obtenir un test de primalité probabiliste.

Proposition 3 : Si n est composé, il y a au plus $\frac{\varphi(n)}{2}$ éléments a premiers avec n tels que $1 \leq a \leq n-1$ et $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} [n]$.

Preuve proposition 1 : "⇐" Supposons $n = p_1 \cdots p_k$, où les p_i sont des nombres premiers distincts, et où $\forall i \in [\![1,k]\!]$, $p_i - 1 \mid n - 1$. Montrons que n est de Carmichael. Soit a un entier premier avec n. Alors pour tout $i \in [\![1,k]\!]$, $a^{p_i - 1} \equiv 1 [p_i]$ d'après le théorème de Fermat (car $a \wedge p_i = 1$ puisque $a \wedge n = 1$), donc comme $p_i - 1 \mid n-1$, on en déduit $a^{n-1} \equiv 1 [p_i]$, ie $p_i \mid a^{n-1} - 1$. Ainsi puisque les p_i sont premiers entre eux, $n = p_1 \cdots p_k \mid (a^{n-1} - 1)$, d'où $a^{n-1} \equiv 1 [n]$.

"⇒" Supposons que n soit un nombre de Carmichael. Montrons tout d'abord que n est sans facteur carré. Supposons par l'absurde $n = p^2 m$ avec p premier. Posons $a = 1 + pm$. D'après le binôme de Newton, $a^p = (1+mp)^p = \sum_{k=0}^{p} \binom{p}{k} m^k p^k$.

Donc $a^p = 1 + mp^2 + m^2p^2 \sum_{k=2}^{p} \binom{p}{k} (mp)^{k-2} \equiv 1 [n]$. L'ordre de a est donc p (cela ne peut pas être 1), donc $p \mid n-1$ (car $a^{n-1} \equiv 1 [n]$) ↯. Donc n est sans facteur carré : $n = p_1 \cdots p_k$ où les p_i sont des premiers distincts. Pour tout $i \in [\![1,k]\!]$, il existe d_i d'ordre $p_i - 1$ dans $(\mathbb{Z}/p_i\mathbb{Z})^\times$ (cyclique). D'après le théorème chinois, il existe $a \in [\![1, n-1]\!]$ tel que $\forall i \in [\![1,k]\!]$, $a \equiv d_i [p_i]$. Alors $a \wedge n = 1$, donc $a^{n-1} \equiv 1 [n]$, et ainsi, $\forall i \in [\![1,k]\!]$, $a^{n-1} \equiv 1 [p_i]$, d'où $p_i - 1 \mid n-1$.

Preuve proposition 2 : "$\Rightarrow$" Supposons $n = p$ premier. (On a alors affaire à des symboles de Legendre "classiques" :)).

On note $\mathbb{F}_p^{*2} = \{y^2, y \in \mathbb{F}_p^*\}$. Alors l'application $\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^{*2}$, $x \longmapsto x^2$ est un morphisme de groupes surjectif de noyau $\{\pm 1\}$.

(± 1 étant les seules racines de $X^2 - 1$ dans le corps $\mathbb{F}_p$, et $1 \neq -1$ car $p \neq 2$). Ainsi d'après le 1er théorème d'isomorphisme (en considérant les cardinaux), on a $\# \mathbb{F}_p^{*2} = \frac{p-1}{2}$.

Notons maintenant $X = \{x \in \mathbb{F}_p, x^{\frac{p-1}{2}} = 1\}$. Alors $|X| \leq \frac{p-1}{2}$ (car le polynôme $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$). D'autre part, si $x \in \mathbb{F}_p^{*2}$ alors $x = y^2$ pour $y \in \mathbb{F}_p^*$, donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$, donc $\mathbb{F}_p^{*2} \subset X$. Ainsi par cardinalité, $X = \mathbb{F}_p^{*2}$. On en déduit alors aussi que $\{x \in \mathbb{F}_p^* \mid x \text{ n'est pas un carré}\} = \{x \in \mathbb{F}_p, x^{\frac{p-1}{2}} = -1\}$ (car $x^{p-1} = 1$ pour $x \in \mathbb{F}_p^*$ donc $x^{\frac{p-1}{2}} = \pm 1$, donc si x n'est pas un carré, $x \notin \mathbb{F}_q^{*2} = X$, donc $x^{\frac{p-1}{2}} = -1$ }). Ainsi pour tout entier a premier avec p, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} [p]$. * possible d'après S_2

"$\Leftarrow$" Supposons que pour tout entier a premier avec n, $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} [n]$, (symbole de Jacobi cette fois) et supposons par l'absurde que n ne soit pas premier. L'hypothèse sur n implique que pour tout entier a premier avec n, $a^{n-1} = \left(\frac{a}{n}\right)^2 = 1 [n]$, donc n est de Carmichael, ainsi $n = p_1 \cdots p_r$ où $r > 1$, les p_i sont des premiers distincts et strictement supérieurs à 2, et où $\forall i \in [\![1, r]\!]$, $p_i - 1 \mid n_i - 1$. On peut alors choisir des entiers $\alpha_1, \dots, \alpha_r$ tels que $\forall i \in [\![1, r-1]\!]$, $\alpha_i \in [\![1, p_i - 1]\!]$ et $\left(\frac{\alpha_i}{p_i}\right) = 1$, et $\alpha_r \in [\![1, p_r - 1]\!]$ tel que $\left(\frac{\alpha_r}{p_r}\right) = -1$ *. D'après le théorème chinois : $\exists! a \in [\![1, n-1]\!]$, $\forall i \in [\![1, r-1]\!]$, $a \equiv \alpha_i [p_i]$. Alors puisque a est premier avec tous les p_i, a est premier avec n, donc par hypothèse, $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} [n]$. Par réduction modulo p_1, on obtient $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} [p_1] = a^{\frac{m(p_1-1)}{2}} [p_1] = \left(\alpha_1^{\frac{p_1-1}{2}}\right)^m [p_1] = \left(\frac{\alpha_1}{p_1}\right)^m [p_1] = 1 [p_1]$

puisque $p_1 - 1 \mid n - 1$

Or d'autre part $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) = -1 [p_1]$. D'où la contradiction.

Preuve proposition 3 : Soit n un entier composé. Alors l'ensemble $\{a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} [n]\}$ est un sous groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$. (il contient $\bar{1}$, et si a_1, a_2 sont dans l'ensemble, alors par multiplicati[vité] du symbole de Jacobi, $\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) = a_1^{\frac{n-1}{2}} a_2^{\frac{n-1}{2}} = (a_1 a_2)^{\frac{n-1}{2}} [n]$, et $\left(\frac{a_1^{-1}}{n}\right) = \left(\frac{a_1}{n}\right) = a_1^{\frac{n-1}{2}} = (a_1^{-1})^{\frac{n-1}{2}} [n]$). D'après la proposition précédente, ce sous groupe est différent de $(\mathbb{Z}/n\mathbb{Z})^\times$ tout entier, or d'après le théorème de Lagrange, son cardinal divise $\varphi(n)$, il est donc inférieur ou égal à $\frac{\varphi(n)}{2}$, ce qui conclut.

On peut déduire de cela un test probabiliste de primalité :
Pour tester si n est premier, on prend un entier a entre 1 et $n-1$ au hasard, puis l'on calcule $\left(\frac{a}{n}\right)$. Si l'on trouve 0, $a \wedge n \neq 1$ donc n n'est pas premier. Sinon on compare $\left(\frac{a}{n}\right)$ à $a^{\frac{n-1}{2}}$. Si c'est différent, alors n est composé, sinon n est probablement premier.
Si n est composé, la proba de ne pas s'en rendre compte après N tests est inférieure à $\frac{1}{2^N}$, c'est touuut petit !

Remarques : * Le critère de Korselt permet de déduire des corollaires concernant les nombres de Carmichael : 1) Si n est un nombre de Carmichael, alors il est impair et composé d'au moins 3 facteurs premiers (n pair $\Rightarrow (-1)^n = 1 [n]$ ↯ et si $n = (a+1)(b+1)$ avec $a \neq b$, alors $n = ab + a + b + 1$ or $a \mid n-1$, donc $a \mid b = (n-1-ab-a)$, de même $b \mid a$ donc $a = b$ ↯)
2) Si $n = pqr$ est de Carmichael avec p fixé, alors q et r sont bornés (c'est de la bricole cf Gourdon).
Les premiers nombres de Carmichael sont $561 = 3 \times 11 \times 17$, $1105 = 5 \times 13 \times 17$, $1729 = 7 \times 13 \times 19$, etc. On sait désormais qu'il y a une infinité de nombres de Carmichael et pour n assez grand, $\#\{m \text{ Carmichael}, m \leq n\} \geq n^{2/7}$.
* Le calcul de $a^{\frac{n-1}{2}}$ se fait en $O(\log(n)^3)$ opérations, et $\left(\frac{a}{n}\right)$ en $O(\log(n)^2)$ opérations, donc au final l'algo est en $O(k \times \log(n)^3)$ où k est le nombre de répétitions de l'algorithme.
* ⚠ Attention aux symboles de Jacobi ! Si $m = a^2 [n]$, alors $\left(\frac{m}{n}\right) = 1$ mais la réciproque est fausse ! (par ex $\left(\frac{14}{51}\right) = 1$ mais 14 n'est pas un carré modulo 51, ce n'est déjà pas le cas modulo 3 !)
* Le théorème de Fermat tel qu'énoncé n'est pas une équivalence, en revanche on a l'équivalence : p est premier $\Leftrightarrow \forall a \in [\![1, p-1]\!], a^{p-1} \equiv 1 [p]$, mais si n est de Carmichael, les seuls témoins de non primalité sont les éléments hors de $(\mathbb{Z}/n\mathbb{Z})^\times$, ce qui devient aussi mauvais qu'un algo "naïf" pour vérifier si n est composé. On pourrait cependant faire un test probabiliste de primalité avec le théorème de Fermat,

mais il serait strictement moins bon que Solovay-Strassen et l'on ne pourrait qu'affirmer "n est probablement premier OU de Carmichael".

* Ici, on n'a que deux sorties à l'algo "n est composé" ou "n est premier avec un risque d'erreur ≤ xxx". Il est beaucoup plus dur de certifier qu'un nombre est premier, ou de le décomposer.

* Il existe un test strictement meilleur que le test de Solovay Strassen : le test de Miller-Rabin (il est aussi ⊕ rapide et ⊕ simple à coder). Soit $n = 1 + 2^s t$ un nombre impair (où t est impair). Alors si $n=p$ est premier, et si a est un entier premier à p, ou bien $a^t \equiv 1 [p]$, ou bien $\exists i \in [\![0, s-1]\!]$, $a^{2^i t} \equiv -1 [n]$ ($a_i := a^{2^i t}$ pour $i \in [\![0, s]\!]$, $a_s = 1$ d'après Fermat, soit tous les a_i valent 1, soit $\exists i \in [\![0, s-1]\!]$, $a_i \neq 1$ et $a_{i+1} = 1$, donc $a_i = -1$ (car X^2-1 a au ⊕ 2 racines)).
Si n est composé, on appelle témoin de Miller un entier a premier avec n tel que $a^t \not\equiv 1 [p]$ et $\forall i \in [\![0, s-1]\!]$, $a^{2^i t} \not\equiv -1 [n]$. On peut montrer que cette condition est strictement plus forte que celle de Solovay-Strassen, et cette fois ci, on peut montrer que le nombre de "menteurs" dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est inférieur à $\frac{1}{4}\varphi(n)$. Donc si on met le test en place, ⊕ des 3/4 des entiers entre 1 et $n-1$ permettent de détecter que n est composé ! (mais bon c'est plus dur alors on va rester sur Solovay Strassen ^^)

* Il existe des tests particuliers pour certains nombres remarquables : le test de Lucas-Lehmer pour les nombres de Mersenne et le test de Pépin pour les nombres de Fermat par exemple.