Test de primalité

L2 Informatique - UFR S.A.T

Pr. Ousmane THIARE

ousmane.thiare@ugb.edu.sn
http://www.ousmanethiare.com

12 septembre 2025

Théorème de Fermat

Test de Miller-Rabin

Tests de Lucas, Selfridge et Pocklington

Test de primalité

Chapitre IV : Test de primalité

Théorème de Fermat

Test de Miller-Rabin

Tests de Lucas, Selfridge et Pocklington

1 Théorème de Fermat

2 Test de Miller-Rabin

3 Tests de Lucas, Selfridge et Pocklington

Théorème de Fermat
Test de Miller-Rabin
Tests de Lucas, Selfridge et Pocklington

Propriété

Petit Théorème de Fermat : Si n est premier et si $a \neq 0, a^n \equiv 1[n]$.

Ce théorème ne peut servir de test de primalité, mais seulement de test de non-primalité. C'est-à-dire que si l'on trouve un nombre $a \not\equiv 0[n]$ tel que $a^{n-1} \not\equiv 1[n]$, on en conclut que n est composé.
Les nombres a tels que $a^{n-1} \equiv 1[n]$ alors que n n'est pas premier ne sont pas nombreux. C'est pourquoi si, après l'essai de quelques valeurs de a, on trouve toujours $a^{n-1} \equiv 1[n]$, ce nombre n sera envoyé à un véritable test de primalité.
Ce pré-test a l'avantage d'être simple et rapide.

Théorème de Fermat

Test de Miller-Rabin

Tests de Lucas, Selfridge et Pocklington

Soit n un nombre impair, que l'on met sous la forme $n-1=2^t m$, avec m impair.

Définition

Ce nombre n est dit pseudo-premier fort dans la base a si l'on peut trouver a tel que :

- *oubien* $a^m \equiv 1[n]$,
- *oubien on peut trouver u tel que* $0 \leq u \leq t-1, a^{2u} m \equiv -1[n]$.

Théorème de Fermat

Test de Miller-Rabin

Tests de Lucas, Selfridge et Pocklington

On montre que :

Propriété

Tout nombre premier est pseudo-premier fort dans n'importe quelle base et qu'un nombre composé est pseudo-premier fort dans au plus $\frac{n}{4}$ bases différentes, et « en général » aucune.

Bien entendu, dès que n est un tant soit peu grand, il est exclu de tester autant de bases.
Il n'en reste pas moins que si, après une dizaine de bases, n est pseudo-premier fort dans chacune de ces bases, il a de « très bonnes chances » d'être premier.
Ce test n'est cependant pas, lui non plus, un véritable test de primalité, mais il est presque aussi rapide que celui de Fermat.

Théorème de Fermat
Test de Miller-Rabin
Tests de Lucas, Selfridge et Pocklington

Le test de Lucas peut s'exprimer de la manière suivante :

Propriété

Si on peut trouver un entier a pour lequel $a^{n-1} \equiv 1[n]$, *mais* $a^{\frac{n-1}{q}} \not\equiv 1[n]$ *pour tous les diviseurs premiers q de n-1, alors n est premier.*

Remarque : Selfridge a montré qu'il n'était pas nécessaire d'utiliser la même valeur de a pour tous ces diviseurs.
Ce test est théoriquement satisfaisant (c'est un test qui peut répondre : « oui, n est premier »), pratiquement il l'est beaucoup moins : il exige la décomposition en facteurs premiers de n-1 qui est une opération en général longue et difficile (voir les algorithmes qui suivent).

Théorème de Fermat

Test de Miller-Rabin

Tests de Lucas, Selfridge et Pocklington

De plus, il connaît un cas d'échec, dans lequel il ne donne pas de réponse.
Le critère de Pocklington permet d'atténuer cette difficulté :

Propriété

Si n n'est que « partiellement décomposé », dans le sens où il a été mis sous la forme n=FR, où F est totalement décomposé en facteurs premiers, mais R n'est pas premier, alors :

- *si le critère de Selfridge appliqué aux diviseurs premiers de F aboutit à un succès,*
- *et si F>R, alors n est premier.*