Algorithme de Rabin-Miller

F. Kany. ISEN-Brest & La Croix-Rouge

Présentation

Soit un entier n.

— Si le test de Rabin-Miller permet d'exhiber un nombre $a \in [2, n-1]$ (appelé témoin de Miller), alors on peut en conclure avec certitude que n n'est pas un nombre premier. (Le nombre a témoigne que n est un nombre composé).

— Si le test de Rabin-Miller ne permet pas d'exhiber un témoin de Miller (après k recherches d'un nombre $a \in [2, n-1]$), alors on peut en conclure avec une très grande probabilité que n est un nombre premier. Cette probabilité peut être rendu aussi proche de 100% que l'on souhaite en augmentant le nombre de recherches k. Malheureusement, on ne peut pas exclure que le nombre n soit premier même si on n'a pas réussit à trouver de témoin de Miller.

  — Si a n'est pas un témoin de Miller, alors on dit que "n est fortement probablement premier en base a".

  — Si a n'est pas un témoin de Miller, mais que n n'est pas un nombre premier, on dit que a est un "menteur fort".

Principe

Lemme [1]
Dans $\mathbb{Z}/p\mathbb{Z}$, si p est premier et si $p > 2$, les seuls nombres X tels que $X^2 \equiv 1 \bmod p$ sont $X = +1$ et $X = -1$.

Proposition [2]
Soit p un nombre premier avec $p > 2$. On a $p-1$ pair et on peut toujours écrire : $p - 1 = 2^s.d$ où s et d sont des entiers et d impair (i.e. s est le nombre maximum de fois que l'on peut mettre 2 en facteur dans $p-1$). Pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^*$, on a :

— soit $a^d \equiv 1 \bmod p$

— soit il existe $r \in [0, s-1]$ tel que $a^{2^r.d} \equiv -1 \bmod p$

Par contraposée, si $\boxed{a^d \not\equiv 1 \pmod n \quad \text{et} \quad \forall r \in \{0, 1, \ldots, s-1\} \quad a^{2^r d} \not\equiv -1 \pmod n}$ alors n est composé et a est un témoin de Miller (que n n'est pas premier).

Exemple

Est-ce que $n = 221$ est premier ? (La réponse est non : $221 = 13 \times 17$)
On a : $n - 1 = 220$ que l'on peut écrire $2^2 \times 55$ (soit $s = 2$ et $d = 55$).
On choisit un nombre $a \in [2, n-1]$ au hasard.

— pour $a = 174$, on calcule :

  — $(a^{2^0})^d \bmod n = 174^{55} \bmod 221 = 47 \neq \pm 1$

  — $(a^{2^1})^d \bmod n = 174^{110} \bmod 221 = 220 = n - 1 = -1 \bmod 221$.

1. Démonstration : $X^2 \equiv 1 \bmod p \Rightarrow (X-1).(X+1) \equiv 0 \bmod p \Rightarrow X = \pm 1 \bmod p$.

2. Démonstration : D'après le petit théorème de Fermat : $a^{p-1} = (a^d)^{2^s} \equiv 1 \bmod p$. En prenant de façon répétée la racine carré de a^{p-1}, on obtient :

— soit $+1 \bmod p$ (jusqu'à $a^d \equiv 1 \bmod p$)

— soit $-1 \bmod p$ (jusqu'à $(a^d)^{2^r} \equiv -1 \bmod p$)

puisque, d'après le lemme, les seules racines possibles sont $+1$ et -1.

Donc 174 n'est pas un témoin de Miller, 221 est fortement probablement premier en base 174. Il faudrait le confirmer en testant d'autres valeurs de a. (En fait, 221 n'est pas premier, 174 est un menteur fort).

— pour $a = 137$, on calcule :
  — $(a^{2^0})^d \bmod n = 137^{55} \bmod 221 = 188 \neq \pm 1$
  — $(a^{2^1})^d \bmod n = 137^{110} \bmod 221 = 205 \neq \pm 1$.

  Donc 137 est un témoin de Miller. 221 n'est pas premier.

Algorithme et temps d'exécution

source `https://fr.wikipedia.org/wiki/Test_de_primalit%C3%A9_de_Miller-Rabin`

La recherche d'un témoin de Miller peut se décrire algorithmiquement de la façon suivante, l'affectation est notée `:=` , `Témoin_de_Miller(a, n)` renvoie

— Vrai si `a` est un témoin de Miller que `n` est composé,

— Faux si `n` est fortement pseudo-premier en base `a`

```
Témoin_de_Miller(a, n):                                  entrées : n un entier impair >=3, a un entier >1
     calculer s et d tels que n - 1 = 2**s * d  avec d impair  s > 0 car n impair
     x := a**d % n    x entier reste de la division de a par n
     si x = 1 ou x = n - 1
       renvoyer(Faux)                                    sortie : a n'est pas un témoin de Miller
     Tant que s > 1
          x := x**2 % n    reste de la division de x**2 par n
          si x = n - 1
            renvoyer(Faux)                               sortie : a n'est pas un témoin de Miller
          s := s - 1
     Fin de boucle tant que
     renvoyer(Vrai)                                      a est un témoin de Miller, n est composé
```

Le test de Miller-Rabin peut alors être décrit comme suit, `Miller_Rabin(n, k)` renvoie

— Vrai si `n` est fortement pseudo-premier en base `a` pour `k` entiers `a`,

— Faux s'il est composé.

```
Miller-Rabin(n,k):                                       entrées : n un entier impair >=3, k un entier >=1
   répéter k fois :
      choisir a aléatoirement dans l'intervalle [2, n-1]
      si Témoin_de_Miller(a,n)
        renvoyer(Faux)                                   sortie, n est composé
   Fin de boucle répéter
   renvoyer(Vrai)                                        sortie, n est probablement premier
                                                                 si k est suffisamment grand
```

La décomposition $n-1 = 2^s.d$ avec d impair se calcule en $O(\log(n))$ par une boucle simple. Ce calcul pourrait être factorisé pour être effectué une seule fois dans le test de Miller-Rabin.

Le calcul du reste de la division a^d par n puis les élévations au carré successives sont des calculs d'exponentiation modulaire. Par exponentiation rapide, le calcul se fait en $O((\log d)(\log n)^2)$ pour le calcul initial, suivi de s ($\leq \log(n)$) élévations au carré en $O((\log n)^2)$. Le temps de calcul du premier algorithme, le test que a est ou non un témoin de Miller pour n est donc en $O((\log n)^3)$. Le temps de calcul du test de Miller-Rabin est donc en $O(k.(\log n)^3)$; ainsi cet algorithme est en temps polynomial et efficace.

Question

1. Coder les fonctions `Temoin_de_Miller(a, n)` et `Miller_Rabin(n,k)`.
2. Tester si 4547337172376300111955330758342147474062293202868155909489 est premier
3. Tester si 4547337172376300111955330758342147474062293202868155909393 est premier

Annexe

On peut rendre le rendre le test de Miller-Rabin déterministe en testant, non pas des valeurs de a aléatoires, mais au contraire un très petit nombre de valeurs de a pré-déterminées.

En pratique :

— pour $n < 2\,047$, il suffit de tester a = 2 ;
— si $n < 1\,373,653$, il suffit de tester a = 2 et 3 ;
— si $n < 9\,080\,191$, il suffit de tester a = 31 et 73 ;
— si $n < 25\,326\,001$, il suffit de tester a = 2, 3 et 5 ;
— si $n < 3\,215\,031\,751$, il suffit de tester a = 2, 3, 5 et 7 ;
— si $n < 4\,759,123\,141$, il suffit de tester a = 2, 7 et 61 ;
— si $n < 1\,122\,004\,669\,633$, il suffit de tester a = 2, 13, 23 et 1662803 ;
— si $n < 2\,152\,302\,898\,747$, il suffit de tester a = 2, 3, 5, 7 et 11 ;
— si $n < 3\,474\,749\,660\,383$, il suffit de tester a = 2, 3, 5, 7, 11 et 13 ;
— si $n < 341\,550\,071\,728\,321$, il suffit de tester a = 2, 3, 5, 7, 11, 13 et 17.