Le test de Miller-Rabin

Marc Lorenzi

12 juillet 2026

1 Introduction

1.1 Notations et rappels

Pour tout $n \in \mathbb{N}^*$, nous noterons $\mathbb{Z}_n$ l'anneau des entiers modulo n, $\mathbb{Z}_n^\times$ le groupe des inversibles de $\mathbb{Z}_n$ et $\mathbb{Z}_n^+ = \mathbb{Z}_n \setminus \{0\}$. Pour tout $x \in \mathbb{Z}$, la classe de x modulo n est

$$x + n\mathbb{Z} = \{x + nk : k \in \mathbb{Z}\}$$

Si p est un nombre premier, alors $\mathbb{Z}_p$ est un corps. Rappelons aussi que si p est un nombre premier différent de 2 et e un entier non nul, le groupe $\mathbb{Z}_{p^e}^\times$ est un groupe cyclique. Son cardinal est

$$\varphi(p^e) = p^{e-1}(p-1)$$

où φ est la *fonction indicatrice d'Euler*.

1.2 Restes chinois

Soit n un entier supérieur ou égal à 2. Écrivons

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

où $r \geq 1$, les p_i sont des nombres premiers distincts et les e_i des entiers non nuls.

Pour tout $m \geq 1$ et tout $x \in \mathbb{Z}$, notons $[x]_m \in \mathbb{Z}_m$ la classe de x modulo m.

Considérons l'application

$$\theta : \mathbb{Z}_n \longrightarrow \mathbb{A} = \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}$$

définie par

$$\theta(x + n\mathbb{Z}) = (x + p_1^{e_1}\mathbb{Z}, \ldots, x + p_r^{e_r}\mathbb{Z})$$

Munissons $\mathbb{A}$ de la structure d'anneau produit (addition et multiplication sont effectuées terme à terme).

Proposition 1. *L'application θ est un isomorphisme d'anneaux.*

Démonstration. Le premier point à vérifier est que θ est bien définie. Soient $x, y \in \mathbb{Z}$. Supposons que $x + n\mathbb{Z} = y + n\mathbb{Z}$, c'est à dire que n divise $x - y$. Pour tout diviseur d de n, d divise alors $x - y$ et donc $x + d\mathbb{Z} = y + d\mathbb{Z}$. En particulier, pour tout $i \in [\![1, r]\!]$, $x + p_i^{e_i}\mathbb{Z} = y + p_i^{e_i}\mathbb{Z}$.

Les propriétés de morphisme de θ sont de simples vérifications.

Soit $a \in \ker \theta$. Posons $a = x + n\mathbb{Z}$ où $x \in \mathbb{Z}$. On a pour tout $i \in [\![1, r]\!]$,

$$x + p_i^{e_i}\mathbb{Z} = 0 + p_i^{e_i}\mathbb{Z}$$

c'est à dire $p_i^{e_i}$ divise x. Les nombres premiers p_i sont distincts deux à deux, donc les entiers $p_i^{e_i}$ sont premiers entre-eux deux à deux. Par le lemme de Gauss, leur produit n divise x. Ainsi, $a = x + n\mathbb{Z} = n\mathbb{Z}$. Le noyau de θ est donc $n\mathbb{Z}$, d'où l'injectivité de θ.

Il reste à remarquer que

$$\left|\prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}\right| = \prod_{i=1}^{r} \left|\mathbb{Z}_{p_i^{e_i}}\right| = \prod_{i=1}^{r} p_i^{e_i} = n = |\mathbb{Z}_n|$$

Les ensembles de départ et d'arrivée de θ sont de même cardinal, d'où la bijectivité de θ. □

Un élément $(a_1, \ldots, a_r)$ de $\mathbb{A}$ est inversible si et seulement si chacun des a_i l'est. Le groupe des inversibles de $\mathbb{A}$ est ainsi

$$\mathbb{A}^\times = \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}^\times$$

La restriction de θ à $\mathbb{Z}_n^\times$ fournit ainsi un isomorphisme de groupes

$$\mathbb{Z}_n^\times \simeq \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}^\times$$

2 Le test de Fermat

Avant d'entrer dans le vif du sujet, commençons par étudier un test de primalité qui s'avérera hélas incorrect.

2.1 Le test

Pour tout entier n impair différent de 1, posons

$$F_n = \{a \in \mathbb{Z}_n^+ : a^{n-1} = 1\}$$

Proposition 2. *F_n est un sous-groupe de $\mathbb{Z}_n^\times$.*

Démonstration. Montrons que F_n est un sous-groupe de $\mathbb{Z}_n^\times$. Soit $a \in F_n$. On a alors $a^{n-1} = 1$, donc a est inversible dans $\mathbb{Z}_n$ et son inverse est a^{n-2}. Ainsi, $F_n \subseteq \mathbb{Z}_n^\times$. Comme $1^{n-1} = 1$, F_n n'est pas vide. Soient $a, b \in F_n$. On a

$$(ab)^{n-1} = a^{n-1}b^{n-1} = 1 \times 1 = 1$$

donc $ab \in F_n$. Enfin, pour tout $a \in F_n$,

$$(a^{-1})^{n-1} = (a^{n-1})^{-1} = 1^{-1} = 1$$

donc $a^{-1} \in F_n$. □

Proposition 3. *Soit n un entier impair différent de 1. Si n est premier alors $F_n = \mathbb{Z}_n^\times$. Si n est composé et $F_n \neq \mathbb{Z}_n^\times$ alors $|F_n| \leq (n-1)/2$.*

Démonstration. Supposons n premier. $\mathbb{Z}_n^+ = \mathbb{Z}_n^\times$ est un groupe d'ordre $n-1$. Par le théorème de Lagrange, pour tout $a \in \mathbb{Z}_n^+$, l'ordre de a divise $n-1$ et donc $a^{n-1} = 1$.

Supposons n composé et $F_n \neq \mathbb{Z}_n^\times$. Par le théorème de Lagrange, $|F_n|$ divise $|\mathbb{Z}_n^\times|$. Il existe donc $c \in \mathbb{N}^*$ tel que

$$|\mathbb{Z}_n^\times| = c|F_n|$$

On a supposé $F_n \neq \mathbb{Z}_n^\times$ donc $c \geq 2$. Ainsi,

$$2|F_n| \leq c|F_n| = |\mathbb{Z}_n^\times| \leq n-1$$

d'où le résultat. □

2.2 Nombres de Carmichael

Existe-t-il des entiers n composés tels que $F_n = \mathbb{Z}_n^\times$? La réponse est hélas oui. Ce sont les *nombres de Carmichael*. Les premiers nombres de Carmichael sont

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585$$

En 1994, Alford, Granville et Pomerance ont montré qu'il existe une infinité de nombres de Carmichael. Dans notre preuve de la correction du test de Miller-Rabin, nous aurons besoin du résultat suivant.

Proposition 4. *Soit n un nombre de Carmichael. Alors $n = p_1 \dots p_r$ où $r \geq 3$ et les p_i sont des nombres premiers distincts.*

Démonstration. Écrivons

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

où $r \geq 2$, les p_i sont des nombres premiers distincts et les e_i des entiers non nuls. Par le théorème des restes chinois, on a un isomorphisme de groupes

$$\mathbb{Z}_n^\times \simeq \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}^\times$$

Les groupes $\mathbb{Z}_{p_i^{e_i}}^{\times}$ sont cycliques d'ordre $\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i-1)$. Supposons que pour tout $a \in \mathbb{Z}_n^{\times}$, $a^{n-1} = 1$. On a alors pour tout $i \in [\![1, r]\!]$ et tout $x \in \mathbb{Z}_{p_i^{e_i}}^{\times}$, $x^{n-1} = 1$ et donc, puisque ces groupes sont cycliques, $p_i^{e_i-1}(p_i-1)$ divise $n-1$. Soit $i \in [\![1, r]\!]$. Remarquons que p_i divise n. En supposant que $e_i > 1$, on a aussi que p_i divise $n-1$. De là, p_i divise 1, contradiction. Ainsi, tous les e_i sont égaux à 1.

Montrons maintenant que $r \geq 3$. Supposons $r = 2$, et donc $n = p_1p_2$. On a

$$n - 1 = p_1p_2 - 1 = (p_1 - 1)p_2 + (p_2 - 1)$$

Comme $p_1 - 1$ divise $n-1$ on a aussi que $p_1 - 1$ divise $p_2 - 1$. De même, $p_2 - 1$ divise $(p_1 - 1)p_2$. Comme p_2-1 est premier avec p_2, par le lemme de Gauss, p_2-1 divise p_1-1. Ainsi, $p_1-1 = p_2-1$ d'où $p_1 = p_2$, contradiction. □

3 Le test de Miller-Rabin

3.1 Introduction

Soit n un entier impair différent de 1. L'entier n s'écrit de façon unique

$$n = t2^h + 1$$

où $t \in \mathbb{N}$ est impair et $h \in \mathbb{N}^*$.

Notons L_n l'ensemble des $a \in \mathbb{Z}_n^+$ vérifiant

- $a^{t2^h} = 1$.
- Pour tout $j \in [\![0, h-1]\!]$, $a^{t2^{j+1}} = 1 \implies a^{t2^j} = \pm 1$.

Définition 1. Pour tout $a \in \mathbb{Z}_n^+$,

- *a passe le test de Miller* si $a \in L_n$.
- a est un *témoin de Miller* si a ne passe passe pas le test de Miller, c'est à adire $a \notin L_n$.

3.2 Existence de témoins de Miller

Nous allons montrer que si n est premier, tous les éléments de $\mathbb{Z}_n^+$ passent le test de Miller. Ou, si l'on préfère, aucun élément de $\mathbb{Z}_n^+$ n'est un témoin de Miller. En revanche, si n n'est pas premier, nous montrerons qu'au moins 3/4 des éléments de $\mathbb{Z}_n^+$ sont des témoins de Miller.

Soit $a \in \mathbb{Z}_n^+$. Remarquons que a est un témoin de Miller si et seulement si

(i) $a^{t2^h} \neq 1$, ou
(ii) il existe $j \in [\![0, h-1]\!]$ tel que $a^{t2^j} \neq \pm 1$ et $(a^{t2^j})^2 = 1$.

Deux cas se présentent.

- Cas 1, pour tout $j \in [\![0, h]\!]$, $a^{t2^j} \neq 1$. Dans ce cas, par (i), a est un témoin de Miller.
- Cas 2, il existe $j \in [\![0, h]\!]$ tel que $a^{t2^j} = 1$. Prenons un tel j minimal, notons-le j_0.

- Cas 2.1, $j_0 = 0$, et donc $a^t = 1$. Dans ce cas, pour tout $j \in [\![0, h]\!]$, $a^{t2^j} = 1$. a n'est donc pas un témoin de Miller.
- Cas 2.2, $j_0 \geq 1$. Si $a^{t2^{j_0-1}} = -1$ alors a est un témoin de Miller. Sinon, par la minimalité de j_0, $a^{t2^{j_0-1}} \neq \pm 1$. De plus, pour tout $j \geq j_0$, $a^{t2^j} = 1$, donc a n'est pas un témoin de Miller.

Commençons par montrer que si n est premier alors n ne possède pas de témoins de Miller.

Proposition 5. *Si n est premier alors $L_n = \mathbb{Z}_n^+$.*

Démonstration. Soit $a \in \mathbb{Z}_n^+$. L'entier n est premier donc, comme nous l'avons vu dans la preuve de la proposition 3,

$$1 = a^{n-1} = a^{t2^h}$$

Soit $j \in [\![0, h-1]\!]$. Supposons que $a^{t2^{j+1}} = 1$. Soit $b = a^{t2^j}$. On a donc $b^2 = 1$, ou encore $(b-1)(b+1) = 1$. Comme $\mathbb{Z}_n$ est un corps, $b = \pm 1$. Ainsi, $\mathbb{Z}_n^+ \subseteq L_n$. L'inclusion réciproque est évidente. □

Nous allons maintenant passer à la partie délicate et montrer que si n n'est pas premier alors il existe beaucoup de témoins de Miller pour l'entier n. Nous allons procéder en deux étapes. Commençons par le cas où n est une puissance d'un nombre premier.

Lemme 6. *On suppose que $n = p^e$ où p est premier impair et $e \geq 2$. Alors,*

$$|L_n| \leq \frac{n-1}{4}$$

Démonstration. Soit $f : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_n^\times$ définie par $f(a) = a^{n-1}$. L'application f est un endomorphisme du groupe $\mathbb{Z}_n^\times$. Le cardinal de $\mathbb{Z}_n^\times$ est $\varphi(n) = p^{e-1}(p-1)$.

Remarquons maintenant que $\ker f$ est l'ensemble des éléments du groupe cyclique $\mathbb{Z}_n^\times$ dont l'ordre divise $n-1$. Par un résultat classique sur les groupes cycliques, le cardinal de $\ker f$ est donc

$$\begin{aligned} |\ker f| &= \text{pgcd}(|\mathbb{Z}_n^\times|, n-1) \\ &= \text{pgcd}(p^{e-1}(p-1), p^e - 1) \\ &= (p-1)\text{pgcd}\left(p^{e-1}, \sum_{k=0}^{e-1} p^k\right) \\ &= p-1 \end{aligned}$$

Clairement, $L_n \subseteq \ker f$. On a donc

$$|L_n| \leq p-1$$

Comme $e \geq 2$,

$$S = \sum_{k=0}^{e-1} p^k \geq 1 + p \geq 4$$

De là,

$$p-1=\frac{p^e-1}{S}=\frac{n-1}{S}\leq\frac{n-1}{4}$$

□

Nous allons maintenant traiter le cas où n n'est pas une puissance d'un nombre premier.

Lemme 7. *On suppose que*

$$n=\prod_{i=1}^{r}p_i^{e_i}$$

où $r\geq 2$, les p_i sont des nombres premiers impairs distincts deux à deux et les e_i sont des entiers non nuls. Alors,

$$|L_n|\leq\frac{n-1}{4}$$

Démonstration. Soit $\theta:\mathbb{Z}_n\longrightarrow\prod_{i=1}^{r}\mathbb{Z}_{p_i{}^{e_i}}$ l'isomorphisme du théorème des restes chinois. Pour tout $i\in[\![1,r]\!]$, posons

$$\varphi(p_i^{e_i})=t_i2^{h_i}$$

où t_i est impair et $h_i\geq 1$. Soit

$$g=\min(h,h_1,\ldots,h_r)$$

Remarquons que $g\geq 1$ et $\mathbb{Z}_{p_i{}^{e_i}}$ est un groupe cyclique d'ordre $t_i2^{h_i}$.

Montrons d'abord que pour tout $a\in L_n$, $a^{t2^g}=1$.

Si $g=h$ c'est immédiat par définition de L_n. Supposons donc $g<h$. Supposons, par l'absurde, que $\alpha^{t2^g}\neq 1$. Soit $j\in[\![g,h-1]\!]$ minimal tel que $a^{t2^{j+1}}=1$. Comme $a\in L_n$ on a alors $a^{t2^j}=-1$.

Comme $g\neq h$, il existe $i\in[\![1,r]\!]$ tel que $g=h_i$. Écrivons

$$\theta(a)=(a_1,\ldots,a_r)$$

On a alors $a_i^{t2^j}=-1$ et aussi $a_i^{t2^{j+1}}=1$. De là, l'ordre de a_i^t dans le groupe multiplicatif $\mathbb{Z}_{p_i{}^{e_i}}$ est 2^{j+1}. Or, $j\geq g=h_i$ donc 2^{j+1} ne divise pas $t_i2^{h_i}$ qui est l'ordre de ce groupe. Contradiction, par le théorème de Lagrange.

Pour tout $j\in[\![0,h]\!]$, soit $\rho_j:\mathbb{Z}_n^\times\longrightarrow\mathbb{Z}_n^\times$ l'application définie pour tout $a\in\mathbb{Z}_n^\times$ par

$$\rho_j(a)=a^{t2^j}$$

Pour tout $a\in L_n$, on a $a^{t2^{g-1}}=\pm 1$. Ainsi, $L_n\subseteq\rho_{g-1}^{-1}(\{\pm 1\})$ et donc

$$|L_n|\leq 2|\ker\rho_{g-1}|$$

Par l'isomorphisme de groupes induit par θ, pour tout $j\in[\![0,h]\!]$,

$$|\ker\rho_j|=\prod_{i=1}^{r}\operatorname{pgcd}(t_i2^{h_i},t2^j)$$

Pour tout $i \in [\![1, r]\!]$, $g \leq h_i$. On a donc

$$\begin{aligned} |\ker \rho_g| &= \prod_{i=1}^{r} \operatorname{pgcd}(t_i 2^{h_i}, t2^g) \\ &= 2^{rg} \prod_{i=1}^{r} \operatorname{pgcd}(t_i 2^{h_i - g}, t) \\ &= 2^{rg} \prod_{i=1}^{r} \operatorname{pgcd}(t_i, t) \end{aligned}$$

où la dernière égalité provient du fait que t est impair. De même,

$$\begin{aligned} |\ker \rho_{g-1}| &= \prod_{i=1}^{r} \operatorname{pgcd}(t_i 2^{h_i}, t2^{g-1}) \\ &= 2^{r(g-1)} \prod_{i=1}^{r} \operatorname{pgcd}(t_i 2^{h_i - g + 1}, t) \\ &= 2^{r(g-1)} \prod_{i=1}^{r} \operatorname{pgcd}(t_i, t) \end{aligned}$$

De là,

$$2^r |\ker \rho_{g-1}| = |\ker \rho_g|$$

Comme $g \leq h$ on a aussi

$$|\ker \rho_g| \leq |\ker \rho_h|$$

De là,

$$|L_n| \leq 2^{-r+1} |\ker \rho_h|$$

Deux cas sont à considérer.

- Cas 1, $r \geq 3$. On a alors
$$|L_n| \leq \frac{1}{4} |\ker \rho_h| \leq \frac{1}{4} |\mathbb{Z}_n^\times| \leq \frac{n-1}{4}$$
- Cas 2, $r = 2$. Par la proposition 4, n n'est pas un nombre de Carmichael et donc $|\ker \rho_h| \leq |\mathbb{Z}_n^\times|/2$. On en déduit ici encore que $|L_n| \leq (n-1)/4$.

□

3.3 Bilan

Pour conclure, nous avons montré le résultat suivant.

Proposition 8. *Soit n un entier impair différent de 1.*

- *Si n est premier, alors $|L_n| = n - 1$.*
- *Si n n'est pas premier alors*
$$|L_n| \leq \frac{n-1}{4}$$

4 Le test de Miller-Rabin en pratique

4.1 Introduction

Dans toute la suite, n désigne un entier premier impair. Le test de Miller-Rabin repose sur la connaissance des deux entiers t, h tels que $n = 1 + t2^h$. La fonction `decomposer` détermine ces deux entiers.

```
def decomposer(n):
    t, h = n - 1, 0
    while t % 2 == 0:
        h = h + 1
        t = t // 2
    return (t, h)
```

La complexité de cette fonction, en nombre d'opérations sur des entiers, est clairement $O(\log n)$.

Maintenant que nous savons calculer t et h, l'étape suivante consiste, pour $a \in \mathbb{Z}_n^+$, à déterminer si a passe le test de Miller. C'est l'objet de la fonction `test_miller`.

```
def test_miller(a, n):
    t, h = decomposer(n)
    b = power_mod(a, t, n)
    for j in range(h):
        if b == n - 1: return True
        if b == 1: return j == 0
        b = (b * b) % n
    return False
```

La fonction `power_mod` renvoie a^t modulo n. En utilisant une exponentiation rapide, cette fonction a une complexité en $O(\log t)$. Comme $t \leq n$, cette complexité est donc aussi en $O(\log n)$. La complexité de `test_miller` est ainsi $O(\log n) + O(h)$. Mais $h \leq \log_2(n)$, donc `test_miller` a une complexité en $O(\log n)$.

Nous pouvons commencer à expérimenter. La figure ci-dessous affiche, pour n impair non premier, le réel $1 - |L_n|/(n-1)$. Par l'étude que nous avons faite, ce réel est au moins égal à $3/4$.

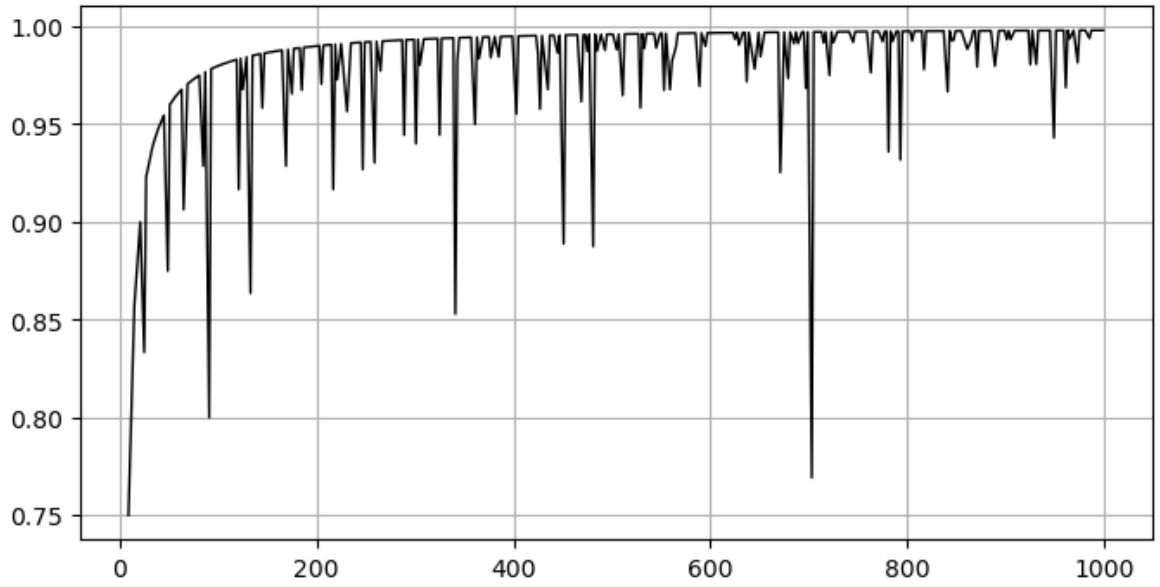

FIGURE 1 – La proportion de témoins de Miller dans $\mathbb{Z}_n$.

On constate que le minorant 3/4 est pessimiste, quoique optimal. La proportion de témoins de Miller est souvent très supérieure à ce minorant.

4.2 Le test de Miller-Rabin

Venons-en au test de primalité de Miller-Rabin proprement dit. Ce test est un *test probabiliste*. Voici une fonction dont nous allons commenter le code. Cette fonction prend en paramètre un entier n impair différent de 1 et un entier N. Elle est censée renvoyer `True` si n est premier et `False` si n est composé. Sa complexité est $O(N \log n)$.

```
1 def premier_miller(n, N):
2     for k in range(N):
3         a = random.randint(1, n - 1)
4         if not test_miller(a, n): return False
5     return True
```

Munissons $\mathbb{Z}_n^+$ de la probabilité uniforme $\mathbb{P}$.

- Supposons tout d'abord n premier. Dans ce cas, il n'existe pas de témoin de Miller pour l'entier n. Le test de la ligne 4 échoue donc toujours. La fonction renvoie donc `True`, ce qui n'est pas pour nous déplaire.
- Supposons maintenant n composé. Le test de la ligne 4 échoue avec une probabilité inférieure à 1/4. La boucle `for` effectue N tirages indépendants d'éléments de $\mathbb{Z}_n^+$. Par l'indépendance des tirages, la probabilité que les N tests de la ligne 4 échouent est le produit des probabilités. Cette probabilité est donc inférieure à $1/4^N$. En passant au complémentaire, la probabilité que cette fonction renvoie `False` est donc supérieure à

$$p_N = 1 - \frac{1}{4^N}$$

Lorsque n est composé, la fonction `premier_miller` peut donc renvoyer une valeur erronée. Cependant, la probabilité d'erreur peut être rendue aussi petite qu'on le désire en prenant N suffisamment grand. Par exemple, pour $N = 10$, la probabilité d'erreur est inférieure à 10^{-6}. Pour $N = 100$, la probabilité d'erreur est inférieure à 10^{-60}.

La discussion qui précède a un défaut certain : elle s'intéresse à la probabilité que notre fonction renvoie la valeur correcte *sachant* que n est premier ou ne l'est pas. Le problème, c'est que c'est exactement le contraire qui nous intéresse : quelle est la probabilité que n soit premier *sachant* que notre fonction renvoie `True` ? Ceci peut être fait rigoureusement mais nous n'en parlerons pas ici. Peut-être une autre fois ?