Test de primalité de Solovay-Strassen

1 Rappels : Anneaux, corps, l'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition 1. *Un anneau est un ensemble A muni de deux opérations une addition $+$ et une multiplication satisfaisant les propriétés suivantes :*

1. *A muni de l'addition est un groupe commutatif d'élément neutre 0.*
2. *La multiplication est associative, possède un élément neutre 1, différent de 0, et elle est distributive par rapport à l'addition, c'est-à-dire que,*

$$\forall x, y, z \in A, \quad x(y+z) = xy + xz.$$

La multiplication n'est pas nécessairement commutative. Si elle l'est on dit que A est un anneau commutatif.

Exercice 1. *Démontrer que si A est un anneau, $x \times 0 = 0 \times x = 0$ pour tout x, et en déduire que 0 n'est pas inversible.*

Solution : Soit $x_0 = x \times 0$. Par distributivité $x_0 + x_0 = x \times 0 + x \times 0 = x \times (0+0) = x \times 0 = x_0$. En ajoutant l'opposé de x_0 aux deux membres de cette égalité on obtient $(-x_0 + x_0) + x_0 = -x0 + x_0$ c'est à dire $0 + x_0 = 0$ et donc $x_0 = 0$. On montre de la même façon que $0 \times x = 0$.

Si x était un inverse de 0 on aurait donc $0 = x \times 0 = 1$ ce qui est exclu par la définition d'un anneau, 1. ∎

Définition 2 (Congruence modulo n.)**.** *Soit n un entier plus grand que 1. Deux a et b appartenant à $\mathbb{Z}$ sont congrus modulo n, et on l'écrit $a \equiv b \pmod{n}$, si et seulement si $b - a$ est un multiple de n.*

La classe de a modulo n est l'ensemble des entiers a' congrus à a modulo n, c'est donc l'ensemble $\{a + n\mathbb{Z}\}$ des entiers obtenus en ajoutant à a un multiple de n. On le note $\overline{a}$. Chacun des élements de $\overline{a}$ est appelé un représentant de cette classe. Deux classes sont disjointes ou confondues. La classe d'équivalence de a coïncide avec la classe du reste de la division euclidienne de a par n. Chaque classe d'équivalence est donc l'un des éléments de l'ensemble $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.

Définition 3. *On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$, des classes d'équivalence modulo n. Muni de l'addition $+$ et de la multiplication définies par*

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a}\overline{b} = \overline{ab},$$

c'est un anneau commutatif de cardinal n.

Ces deux définitions ont un sens parce que si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$ alors $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$; autrement dit les classes $\overline{a+b}$ et $\overline{ab}$ ne dépendent pas des représentants a et b choisis dans chacune des classes $\overline{a}$ et $\overline{b}$.

On rappelle qu'un corps est un anneau dont tout élément non nul est inversible, c'est à dire tel que pour tout $x \neq 0$ appartenant à A il existe un y de A tel que $xy = yx = 1$.

Définition 4. *L'anneau A est intègre s'il ne contient pas de diviseur de 0, c'est à dire si le produit de deux éléments non nuls n'est jamais nul.*

Proposition 1. *Pour qu'un anneau soit un corps il est nécessaire mais non suffisant qu'il soit intègre.*

Démonstration: Si A n'est pas intègre, il existe a et b non nuls tels que $ab = 0$. Si a admettait un inverse a' on en déduirait que $0 = a' \times 0 = a' \times (ab) = (a'a) \times b = 1 \times b = b$. Ce qui contredit l'hypothèse $b \neq 0$.

Mais l'intégrité de l'anneau A ne suffit pas à faire de celui-ci un corps. $\mathbb{Z}$ par exemple est intègre mais tout $x \neq \pm 1$ n'est pas inversible. ■

Le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2. *L'élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a est premier avec n. Autrement dit :*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid a \in \mathbb{Z}, \operatorname{pgcd}(a,n) = 1\}.$$

Démonstration: C'est une conséquence immédiate du théorème de Bezout. En effet, $\overline{a}$ est inversible si et seulement si il existe u tel que $\overline{a} \times \overline{u} = \overline{1}$, autrement dit s'il existe u et v tels que $au - 1 = nv$, soit $au - nv = 1$. ■

Théorème 1. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Démonstration: Si n n'est pas premier, il existe $2 \leq a \leq b < n$ avec $ab = n$. On a donc $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$ et $\overline{a} \times \overline{b} = \overline{n} = 0$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est donc pas intègre.

Si p est premier, tous les entiers $1 \leq a \leq p-1$ sont inversibles car premiers avec p, tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont donc inversibles. ■

Théorème 2 (**Petit théorème de Fermat**). *Si p est premier et a non multiple de p on a*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Théorème 3 (**Théorème de Wilson**). *Pour que p soit premier, il faut et il suffit que*

$$(p-1)! \equiv -1 \pmod{p}.$$

Démonstration: Si p n'est pas premier $p = ab$, $2 \leq a \leq b \leq p-1$. Il en résulte que $(p-1)!$ est un multiple de $ab = p$ donc congru à 0 modulo p.

Si p est premier les seuls éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux avec leur inverse sont $\overline{1}$ et $\overline{p-1} = \overline{-1}$. En effet l'équation $x^2 = \overline{1}$ s'écrit encore $(x-\overline{1})(x+\overline{1}) = 0$ qui implique $x = \overline{1}$ ou $x = \overline{-1}$. Réordonnons les termes du produit $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$ en plaçant en première position 1 et $p-1$ et plaçant chacun des autres à côté de son inverse modulo p, on obtient la congruence :

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (x_1 \cdot x_1^{-1}) \cdot \ldots (x_k \cdot x_k^{-1}) \equiv -1 \pmod{p}.$$

2 Le symbole de Legendre

Définition 5. *Soit n un entier naturel non nul. On dit que l'entier relatif a est un résidu quadratique modulo n s'il existe un entier x tel que*

$$x^2 \equiv a \pmod{n},$$

c'est à dire si l'élément $\overline{a} = \overline{x}^2$ de $\mathbb{Z}/n\mathbb{Z}$ est un carré.

Proposition 3. *Il y a exactement $(p-1)/2$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration: Tout élément de $\mathbb{Z}/p\mathbb{Z}$ est la classe d'un $x \in [\![-(p-1)/2, (p-1)/2]\!]$. Puisque le carré de $-x$ est le même que celui de x, chaque carré non nul s'écrit $\overline{x}^2$ avec $x \in [\![1, (p-1)/2]\!]$, et cette écriture est unique car la congruence $x^2 \equiv x'^2 \pmod{p}$ s'écrit

$$(x'-x)(x'+x) \equiv 0 \pmod{p}$$

et implique $x = x'$ ou $x' + x = kp \geq p$, ce qui est incompatible avec $x, x' \leq (p-1)/2$.

Définition 6. *Le symbole de Legendre de a modulo p, noté $\left(\frac{a}{p}\right)$ est défini pour tout entier a et tout nombre premier p impair, par*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \text{ est un multiple de } p \\ +1 \text{ si } a \text{ non multiple de } p \text{ est un carré modulo } p \\ -1 \text{ si } a \text{ non multiple de } p \text{ n'est pas un carré modulo } p \end{cases}$$

Théorème 4. *Le critère d'Euler. Si p est un nombre premier impair n*

$$\forall a \in \mathbb{Z}, \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{2}$$

Démonstration: Si a est multiple de p, $\left(\frac{a}{p}\right) = 0$ et $a^{p-1} \equiv 0 \pmod{p}$, l'égalité (2) est donc satisfaite. Supposons maintenant a non multiple de p.

Si $a \equiv x^2 \pmod{p}$ est un résidu quadratique, $a^{(p-1)/2}$ est congru à x^{p-1}, donc à 1 grâce au petit théorème de Fermat.

Si a n'est pas un carré modulo p, pour tout x non mutiple de p, l'équation $xy \equiv a \pmod{p}$ possède une unique solution y modulo p, $y = x^{-1}a$, où x^{-1} est un inverse de x modulo p. Et cette solution y n'est pas congrue à x modulo p car a n'est pas un carré modulo p. En regroupant ainsi les $p-1$ termes du produit $(p-1)!$ en $(p-1)/2$ paires $\{x, y\}$, solutions de $xy \equiv a \pmod{p}$, On obtient

$$(p-1)! \equiv (x_1 \cdot y_1) \cdot (x_2 \cdot y_2) \cdot \cdots \cdot (x_{(p-1)/2}, y_{(p-1)/2}) \equiv a^{(p-1)/2} \pmod{p}.$$

et la conclusion car, grâce au théorème de Wilson, $(p-1)! \equiv -1 \pmod{p}$. ∎

Proposition 4. *Le symbole de legendre est multiplicatif en a, c'est à dire que, pour tous a, b*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Démonstration: Cela résulte immédiatement du critère d'Euler, qui donne

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

∎

Proposition 5 (Lemme de Zolotarev.)**.** *Soit Soit p un nombre premier impair et a non multiple de p. Puisque $\overline{a}$ est inversible, la multiplication par $\overline{a}$, $\mu_{\overline{a}} : x \longrightarrow \overline{a}x$, est une permutaion de $(\mathbb{Z}/p\mathbb{Z})^\times$, et le symbole de Legendre $\left(\frac{a}{p}\right)$ est la signature de cette permutation :*

$$\left(\frac{a}{p}\right) = \varepsilon(\mu_{\overline{a}}).$$

Démonstration: On définit les applications ψ et $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{-1, 1\}$, par $\psi(\overline{a}) = \left(\frac{a}{p}\right)$ et $\phi(\overline{a}) = \varepsilon(\mu_{\overline{a}})$. La première, ψ_a est multiplicative par multiplicativité

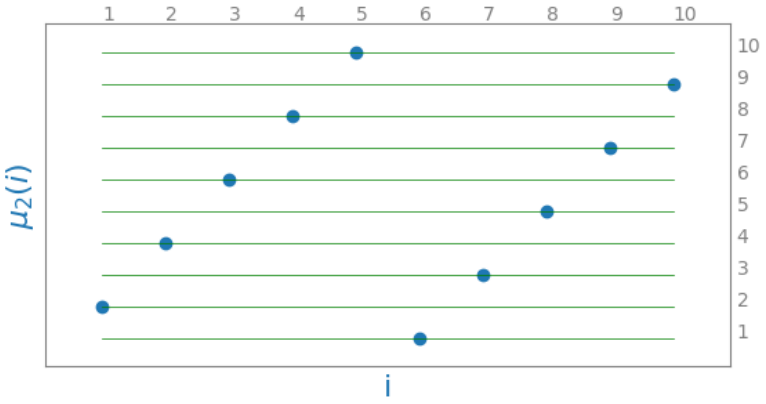

FIGURE 1 – Graphe de la multiplication par 2 dans $(\mathbb{Z}/11\mathbb{Z})^\times$

en a de $\left(\frac{a}{p}\right)$. La seconde, ϕ est, elle aussi, multiplicative, car la signature de $\mu_{\overline{ab}} = \mu_{\overline{a}} \circ \mu_{\overline{b}}$ est le produit des signatures de $\mu_{\overline{a}}$ et $\mu_{\overline{b}}$. Soit g un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors $\psi(g) = \left(\frac{g}{p}\right) = -1$ car g n'est pas un carré.

Puisque $g^{p-1} = 1$, μ_g est le cycle $(1, g, \ldots, g^{p-2})$. C'est donc un cycle d'ordre pair $p-1$, sa signature est donc -1. Enfin, les deux applications ϕ et ψ sont multiplicatives et coïncident sur le générateur g elles sont donc identiques. ∎

Du critère d'Euler, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/4} \pmod p$ on déduit immédiatement, la proposition :

Proposition 6. *Le symbole de Legendre de -1 ne dépend que de la classe de p modulo 4,*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p = 4k+1 \\ -1, & p = 4k+3 \end{cases}$$

Le symbole de Legendre de 2, ne dépend, lui, que de la classe de p modulo 8.

Proposition 7. *Le symbole de Legendre $\left(\frac{2}{p}\right)$ est donné par*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{si p} \equiv 1 \quad \text{ou} \quad \text{p} \equiv 7 \pmod 8 \\ -1, & \text{si p} \equiv 3 \quad \text{et} \quad \text{p} \equiv 5 \pmod 8 \end{cases} \tag{3}$$

Démonstration:

Par le lemme de Zolotarev $\left(\frac{2}{p}\right)$ est la signature de la substitution $x \mapsto 2x$ de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Considérons par exemple, $p = 11$. La figure 2 montre le graphe de μ_2. L'ensemble des inversions de μ_2 est $\{(i,j) \mid i < j,\ \mu_2(i) > \mu_2(j)\}$. Partitionnons cet ensemble de couples selon la valeur de i, déterminons le nombre $inv(i)$ des inversion des couples (i,j) de premier terme i.

Pour $i = 1, \mu_2(i) = 2$; il faut compter les $j > 1$ tels que $\mu_2(j) < 2$. Il n'y en qu'un c'est $i = 6$, avec $\mu_2(6) = 1$. $inv(1) = 1$.

Pour $i = 2, \mu_2(i) = 4$; il faut compter les $j > 1$ tels que $\mu_2(j) < 4$. Il y en a 2, 6, et 7 avec $\mu_2(7) = 3$; et donc $inv(2) = 3$.

Et ainsi de suite, $inv(4) = 4$, $inv(5) = 5$. Et, à partir de $i = 6 = (p+1)/2$ il n'y a pas de nouvelle inversion car μ_2 st croissante sur l'intervalle $[6 - 10]$.

Dans le cas général le nombre des inversions de μ_2 est $1 + 2 + \cdots + (p-1) = (p^2-1)/8$ qui est pair si et seulement si $p \equiv \pm 1 \pmod 8$. ■

Donnons enfin, sans démonstration, la loi de réciprocité quadratique, publiée par Gauss en 1801.

Théorème 5 (Loi de réciprocité quadratique). *Si p et q sont deux nombres premiers impairs les symboles de Legendre $\left(\frac{p}{a}\right)$ et $\left(\frac{q}{p}\right)$ sont liés par*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)/2}(-1)^{(q-1)/2}\left(\frac{q}{p}\right).$$

Le coefficient $(-1)^{(p-1)/2}(-1)^{(q-1)/2}$ est 1 sauf dans le cas où p et q sont tous deux congrus à 3 modulo 4.

3 Le symbole de Jacobi

Le symbole de Jacobi prolonge la défintion du symbole de Legendre en l'étendant à tout couple d'entiers naturels (a,n), avec n impair. Lorsque n est premier, il coïncide avec le symbole de Legendre ; on peut donc le représenter par la même notation que celui-ci sans créer d'ambiguïté.

Définition 7. *Soit a un entier arbitraire et n, impair, $n = \prod_{i=1}^{k} p_i$ où les p_i sont premiers. Le symbole de Jacobi $\left(\frac{a}{b}\right)$ est le produit des symboles de Legendre $\left(\frac{a}{p_i}\right)$*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right).$$

Les propriétés du symbole de Legendre s'étendent au symbole de Jacobi.

Proposition 8. *Propriétés du symbole de Jacobi*

1. $\left(\frac{a}{n}\right) = 0$ *si et seulement si* a *n'est pas premier avec* n.
2. *Périodicité :* $\left(\frac{a}{n}\right)$ *ne dépend que de la classe* a *modulo* n.
3. *Multiplicativité :* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ *et* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
4. *Règle* $a = 2$ *:* $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1, & \text{si n} \equiv 1 \quad \text{ou} \quad \text{n} \equiv 7 \pmod 8 \\ -1, & \text{si n} \equiv 3 \quad \text{et} \quad \text{n} \equiv 5 \pmod 8 \end{cases}$
5. *Réciprocité quadratique : Si* a *et* b *sont impairs*

$$\left(\frac{a}{b}\right) = (-1)^{(a-1)/2}(-1)^{(b-1)/2}\left(\frac{b}{a}\right).$$

La loi de réciprocité quadratique appliquée au calcul de $\left(\frac{a}{b}\right)$, avec la périodicité donne pour tous a et b impairs, $0 < a < b$ la formule $\left(\frac{a}{b}\right) = (-1)^{(a-1)/2}(-1)^{(b-1)/2}\left(\frac{r}{a}\right)$, où r est le reste de la division de b par a.

On en déduit immédiatemment l'algorithme suivant qui n'utilise la multiplicativité que lorsque a est pair. Quand il est impair on utilise la proposition ce-dessus. Ce qui nous conduit à l'algorithme suivant très proche de l'algorithme d'Euclide.

```
1  def jacobi(a,b):
2      """ Calcul de jacobi (a,b) pour 0 <= a < b avec b impair """
3      res = 1
4      while a > 0:
5          while a % 2 == 0:
6              if (b % 8) != 1 and  (b % 8) != 7:
7                res = -res
8              a //= 2
9          if a % 4 == 3 and  b % 4 == 3:
10             res = -res
11         r = b % a
12         a , b = r , a
13     if b == 1: # pgcd(a,b) = 1
14         return res
15     else: # pgcd(a,b) > 1
16         return 0
```

Théorème 6 (Solovay-Strassen). *L'entier impair $n \in \mathbb{N}$, est premier si et seulement si il satisfait le crirère d'Euler, c'est à dire si pour tout a premier avec n :*

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}. \tag{4}$$

Démonstration: Cette condition est nécessaire, c'est le Theorème 4.

Par contraposition, démontrons que si n n'est pas premier il existe un entier a premier avec n tel que $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$. Distinguons deux cas :

1. Si n est sans facteur carré, c'est un produit de nombres premiers deux à deux distincts, soit p l'un d'entre eux, et $q = n/p$. Choisissons d'abord u non carré modulo p. Puisque $\text{pgcd}(p, q) = 1$, par le théorème des restes chinois, il existe a tel que :
$$a \equiv u \pmod{p} \quad \text{et} \quad a \equiv 1 \pmod{q} \tag{5}$$
Vu la multiplicativité en b du symbole de jacobi $\left(\frac{a}{b}\right)$
$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \times \left(\frac{a}{q}\right) = \left(\frac{u}{p}\right) \times \left(\frac{1}{q}\right) = -1.$$
Puisque n est multiple de a, la congruence $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ impliquerait $a^{\frac{n-1}{2}} \equiv -1 \pmod{q}$. Ce qui est exclu car $a \equiv 1 \pmod{q}$.
2. Sinon on peut écritre $n = p^\alpha q$, avec $\alpha \geq 2$ et $\text{pgcd}(p, q) = 1$. Choisissons $a = 1 + p^{\alpha-1}q$. Par multiplicativité du symbole de jacobi on a :
$$\left(\frac{a}{n}\right) = \left(\frac{a}{p^\alpha q}\right) = \left(\frac{a}{p}\right)^\alpha \left(\frac{a}{q}\right) = 1$$
car a est congru à 1 modulo p et q. Si $a^{(n-1)/2}$ était congru à 1 modulo n, qui est un multiple de p^α il serait aussi congru à 1 modulo p^α.
Développons $a^{(n-1)/2} = (1 + p^\alpha q)^{(n-1)/2}$ par la formule du binôme. Tous les termes, à partir du troisième sont nuls modulo p^α, car $2(\alpha - 1) \geq \alpha$, et donc
$$a^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} p^{\alpha-1} q \pmod{p^\alpha}.$$
La plus grande puissance de p qui divise $a^{\frac{n-1}{2}} - 1$ est donc $p^{\alpha-1}$. Ce nombre $a^{\frac{n-1}{2}}$ n'est donc pas congru à 1 modulo p^α.

Soit n un entier impair. Un entier a satisfaisantt $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ nous incite à conjecturer que n est premier. D'où la définition suivante.

Définition 8. *Soit n un entier impair non premier. On dit que a est un faux témoin de primalité de n si* $\mathrm{pgcd}(a,n)=1$ *et*

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

c'est à dire si dans $\mathbb{Z}/n\mathbb{Z}$ on a l'égalité $\overline{\left(\frac{a}{n}\right)} = \overline{a}^{\frac{n-1}{2}}$.

Proposition 9. *Soit n impair non premier. Le nombre de ses faux témoins dans l'intervalle $\{1,2,\ldots,n-1\}$ est plus petit que $n/2$. Autrement dit, si on choisit a au hasard, avec quiprobabilité dans $\mathbb{Z}/n\mathbb{Z}-\{0\}$, la probabilité pour que a soit un faux témoin de primalité de n est plus petite que $1/2$.*

Démonstration: La congruence $\left(\frac{a}{n}\right) \equiv \overline{a}^{\frac{n-1}{2}}$ équivaut à $\overline{\left(\frac{a}{n}\right)}\overline{a}^{\frac{n-1}{2}} \equiv \overline{1}$ parce que $\left(\frac{a}{n}\right) \equiv \pm 1$ est son propre inverse. L'application $\psi : \overline{a} \mapsto \overline{\left(\frac{a}{n}\right)}\overline{a}^{\frac{n-1}{2}}$ est multiplicative car c'est le produit de deux fonctions multiplicatives. C'est donc un endomorphisme du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, et a est un faux témoin si et seulement si $\overline{a}$ appartient à $\ker(\psi)$. Le théorème de Solovay-Strassen dit qu'il existe des entiers qui ne sont pas des faux témoins ; $\ker(\psi)$ est donc un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^\times$. Son cardinal est ainsi un diviseur de $\mathrm{card}\,(\mathbb{Z}/n\mathbb{Z})^\times$, donc majoré par $\mathrm{card}\,(\mathbb{Z}/n\mathbb{Z})^\times/2 \leq (n-1)/2$.

Test de Solovay Strassen

1. On choisit un entier k et on répète au plus k fois :
2. On tire au hasard a entre 1 et $n-1$. Si $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$ on a prouvé que n n'est pas premier, et on s'arrête là.
3. Si aucun des k tirages n'a permis de conclure, on n'a rien prouvé, mais, si n est premier, la probabilité de cet évènement était inférieure à 2^{-k}.

Pour implémenter le test de Solovay-Strassen il faut calculer rapidement les $a^k \pmod{n}$, les exponentielles modulo n. Commençons par ce point.

L'exponentiation rapide

Soit k et x deux entiers non nuls. On peut calculer $k \times x$ de la manière suivante : on écrit k et x sur une première ligne. Puis, sur la ligne suivante, on remplace k par sa moitié et x par $x+x$. Et ainst de suite jusqu'à obtenir $k=1$. Pour calculer

$19 \times 23 = \underbrace{23 + 23 + \cdots + 23}_{19}$ on écrit donc :

k	x
19	23
9	46
4	92
2	184
1	368

On obtient le produit cherché en additionnant les nombres de la colonne des x qui figurent à droite d'une valeur impaire de k. Pour cet exemple ce sont 23, à droite de 19, 46, à droite de 9 et 368 à droite 1. Ce qui donne

$$19 \times 23 = 23 + 46 + 368 = 437.$$

Explication : l'écriture de k en base 2. Rajoutons une colonne à gauche dans laquelle on écrit 0 ou 1 selon que la valeur de k est paire ou impaire.

	c	k	x
1	1	19	23
2	1	9	46
4	0	4	92
8	0	2	184
16	1	1	368

Les nombres de la colonne c sont, en partant du chiffre des unités, les chiffres de l'écriture en base 2 de 19. D'où

$$19 = 1 + 2 + 16 \text{ et } 19 \times 23 = 1 \times 23 + 2 \times 23 + 16 \times 23 = 437.$$

Le même algorithme permet de calculer rapidement l'expression :

$$x * x * x * \cdots * x$$

dans laquelle x figure k fois et $*$ est une opération binaire associative quelconque.

Remplaçant l'opérateur $*$ par la multiplication modulo n : $(x, y) \longrightarrow (x * y) \,\%\, n$, nous obtenons la fonction python expMod qui calcule x^k modulo n.

Nous disposon maintenant de tous les éléments pour implémenter le test de Solovay-Strassen.

```python
def expMod(x,k,n):
    """ Calcul de x^k modulo n """
    res = 1
    while k > 0:
        if k % 2 == 1:
            res = (res * x) % n
        k = k // 2
        x = (x * x) % n
    return res
```

```python
def solovayStrassen(n,k):
    for i in range(k):
        a = random.randint(1,n-1)
        d = gcd(a, n)
        if d > 1:
            return False
        j = jacobi(a,n)
        r = expMod(a,(n-1)//2,n)
        if (r - j) % n  != 0:
            return False
    print("Non prouvé mais n est certainement premier")
    return True
```

Application : Calcul de grands nombres pseudo-premiers

```python
def next_pseudo_prime(x, k=100):
    """ Renvoie le plus petit pseudo-premier >= x """
    if x % 2 == 0:
        x += 1
    while not solovayStrassen(x,k):
        x += 2
    return x
```

```
%%time
x = 10**499
next_pseudo_prime(x)
```

```
CPU times: user 2.93 s, sys: 4.77 ms, total: 2.93 s
Wall time: 2.93 s
```

```
10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000153
```

FIGURE 2 – Le plus petit nombre premier de 500 chiffres décimaux