Tests de primalité probabilistes

Baptiste DAUMEN : Numéro candidat 496

Juin 2021

1 Introduction

Actuellement, de nombreux systèmes de cryptographie utilisent des nombres premiers. Un des systèmes les plus connus étant celui le RSA. Ce système est notamment utilisé pour crypter des informations sur Internet et sécuriser des transferts d'argent électronique. La performance de ces systèmes de protection est donc un enjeu sociétal très important. Ces chiffrements utilisent des nombres premiers, de très grands nombres premiers, qu'il faut pouvoir générer de façon optimale en ayant la certitude, ou tout du moins une probabilité très importante, qu'il soit premier . Or les tests de primalité déterministes sont extrêmement coûteux en complexité temporelle (complexité exponentielle en la taille du nombre). Il faut donc trouver des algorithmes performants qui donnent avec une certaine probabilité si un nombre est premier ou non. En effet à partir d'une certaine probabilité donnée qu'un nombre soit premier, on peut se satifaire de l'utilisation de ce nombre dans les systèmes de cryptage tel que le RSA.

2 Test de primalité de Fermat

Le test de primalité de Fermat repose sur le petit théorème de Fermat.

Théorème 1 (De Fermat - petit)**.** $\forall\ p \in \mathcal{P}$ *et* $\forall\ a \in Z$ *tel que* $a \wedge p = 1$ *alors* $a^{p-1} \equiv 1\ [p]$.

Démonstration. Le groupe $\mathcal{G}$ des inversibles de Z/pZ est de cardinal $p-1$ donc l'ordre de tout élément $\bar{a}$ divise $p-1$. D'où le résultat. □

Explication du test : Si on veut tester la primalité de n alors on choisit a premier avec n, en pratique $a \in [|1, n-1|]$ car on suppose n premier, et on calcule le reste de la division euclidienne de a^{n-1} par n. Si on a 1 alors n peut être premier, sinon on est sûr qu'il est composé. La complexité de l'algorithme associé au test est en $O(log(n))$

Problème lié au test : Un défaut majeur de ce test et qu'il existe des nombres n non premiers qui vérifient $\forall\, a \in Z$ tel que $a \wedge n = 1 : a^{n-1} \equiv 1\ [n]$. Ces nombres sont appelés nombre de Carmichael. Le premier d'entre-eux est 561. Pour cette raison, le test de Fermat n'est pas utilisé car il n'est pas fiable. On peut vérifier que 561 est un nombre de Carmichael en utilisant un programme informatique.

Nombres de Carmichael : Ces nombres prouvent donc que la réciproque du petit théorème de Fermat est fausse. Or on peut se demander s'il existe un nombre fini de nombres de Carmichael, ce qui permettrait d'utiliser le test de Fermat pour des nombres premiers supérieurs assez grand (supérieur au plus grand nombre de Carmichael).

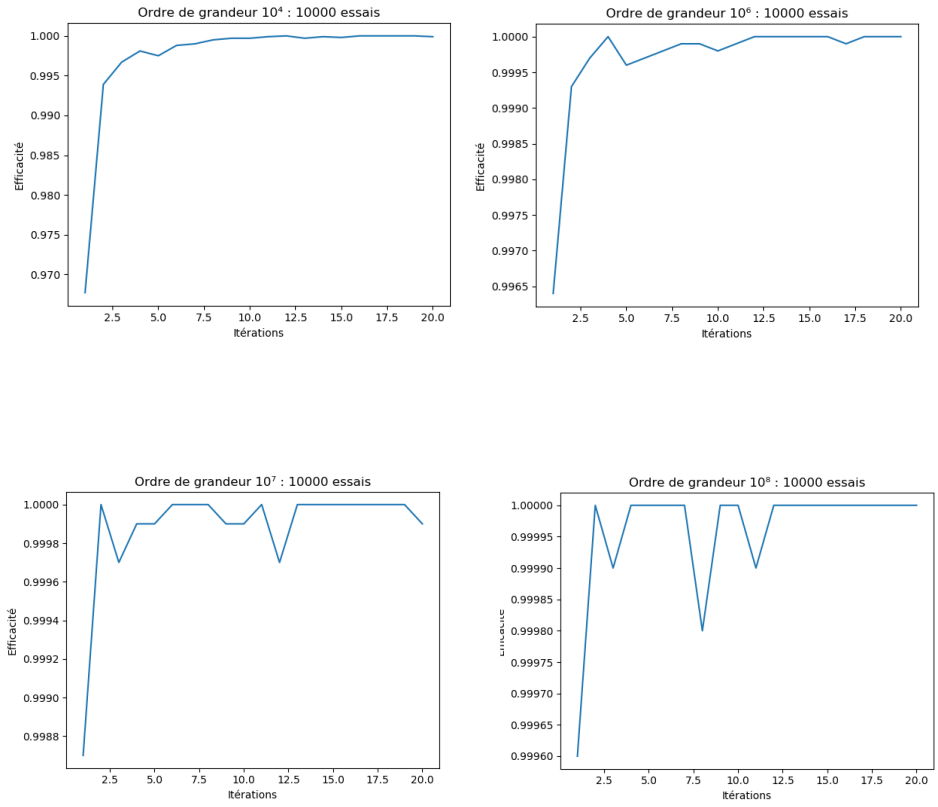

FIGURE 1 – 3 images side by side, OMG

3 Test de Miller-Rabin

Le test de Miller-Rabin se base aussi sur le petit théorème de Fermat.

Propriété 1. *Soit $p > 2$ premier ; on écrit $p - 1 = 2^s t$, avec t impair et $s = v_2(p-1) \geq 1$ Soit a premier avec p alors $a^t \equiv 1\ [p]$ ou $\exists\ j \in [|0, s-1|]$ tel que $a^{2^j t} \equiv -1\ [p]$.*

Explication du test Le test de Miller-Rabin consiste à choisir aléatoirement a dans $[|1, n-1|]$ et tester s'il vérifie la propriété de Miller-Rabin. Ce test peut-être effectué à plusieurs reprises pour obtenir une probabilité importante que n soit premier. La complexité de l'algorithme associé au test est en $O(log(n)^3)$.

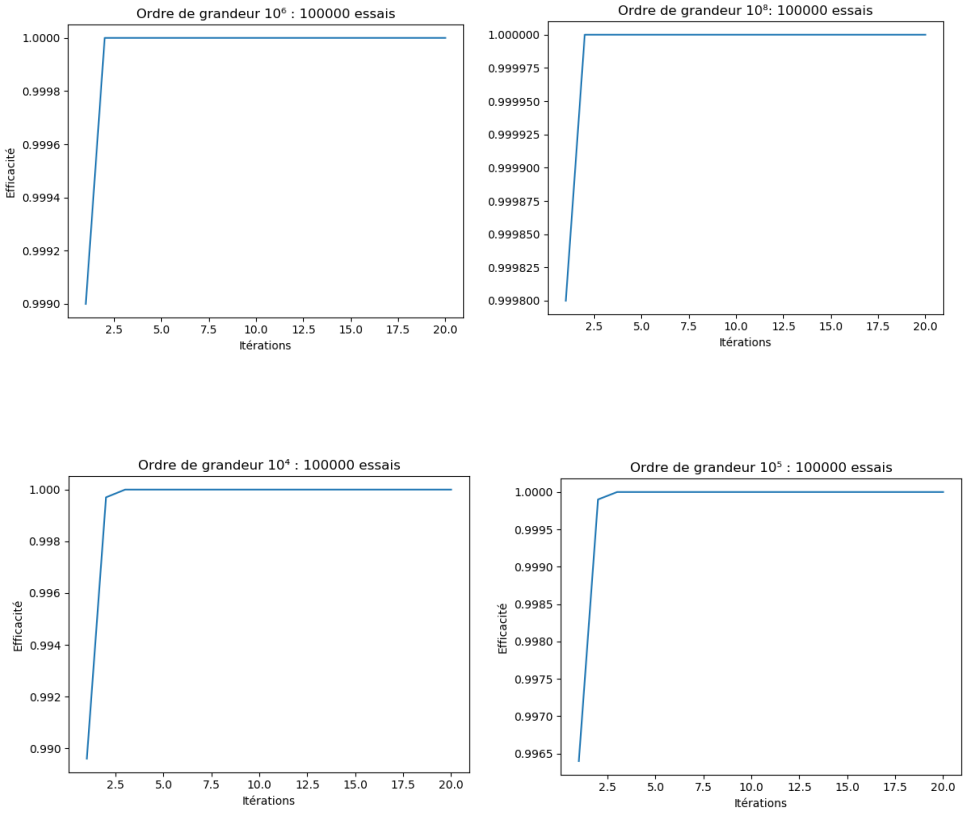

FIGURE 2 – 3 images side by side, OMG

On s'intéresse à connaître la répartition des témoins du test de Miller-Rabin.

Théorème 2. *Soit n un entier composé impair et $n > 9$. On a $n-1 = 2^\alpha m$ avec m impair. On note $\mathcal{S} = \{x \in Z/nZ^* \text{ tel que } x^m \equiv 1\ [p] \text{ ou } \exists\ j \in [|0, \alpha-1|] \text{ tel que } x^{2^j m} \equiv -1\ [p]\}$.*
Alors $\frac{\#\mathcal{S}}{\varphi(n)} \leq \frac{1}{4}$

Lemme 1. *a et b deux éléments d'un groupe G. Si $ord(a) = n$ et $ord(b) = m$ et $n \wedge m = 1$ alors $ord(ab) = nm$.*

Lemme 2. *Si G est un groupe cyclique alors tout sous groupe H est cyclique.*

Lemme 3. *Soit G un groupe cyclique de cardinal m. Le nombre d'éléments d'ordre d pour $d \mid m$ est $\varphi(d)$.*

Lemme 4. *Pour tout p premier impair et pour tout $n \in N^*$, le groupe Z/p^nZ^* est cyclique de cardinal $p^{n-1}(p-1)$.*

Démonstration. Si $n = 1$ alors Z/pZ est un corps. Pour tout diviseur d de $p-1$, on note $f(d)$ le nombre d'éléments de Z/pZ^* d'ordre d. Supposons qu'il existe un élément a d'ordre d, un diviseur de $p-1$. a engendre un sous-groupe $H =< a >$ de cardinal d. Les éléments de H sont racines du polynôme $P = X^d - 1$. Or Z/pZ est un corps donc P a au plus d racines. Donc les racines de P sont les éléments de H. Or les éléments d'ordre d de Z/pZ sont les racines de P donc les éléments de H. Le nombre d'éléments d'ordre d est le nombre de générateurs de H donc $\varphi(d)$. Donc $f(d) = \varphi(d)$ ou $f(d) = 0$. Or p-1 $= \sum_{d|p-1} \varphi(d) = \sum_{d|p-1} f(d)$. On en déduit $\varphi(d) = f(d)$. Pour $d = p-1$, il vient $f(p-1) = \varphi(p-1) > 0$. Il existe un élément d'ordre $p-1$ donc Z/pZ^* est cyclique.

Si $n \geq 2$: on recherche un élément d'ordre p^{n-1} (1) et un d'ordre $p-1$ (2).
(1) : Par récurrence finie, montrons que pour $m \in [|1, n-1|]$ on a $(1+p)^{p^m} = 1 + p^{m+1}u_{m+1}$ avec p ne divise pas u_{m+1}.

Pour $m = n-1$: $(1+p)^{p^{n-1}} = 1 + p^n u_n$ alors $(1+p)^{p^{n-1}} \equiv 1\ [p^n]$. Donc $ord(\overline{1+p}) \mid p^{n-1}$ dans Z/p^nZ^*. Or p est premier donc $\exists k \in [|1, n-1|]$ tel que $ord(\overline{1+p}) = p^k$.
Si $k \geq 2$, $(1+p)^{p^k} = 1 + p^{k+1}u_{k+1}$ et $k+1 \geq n-1$ et p ne divise pas u_{k+1} donc $(1+p)^{p^k} \not\equiv [p^n]$. Donc $ord(\overline{1+p}) = p^{n-1}$. Le résultat attendu.

(2) : Le morphisme d'anneaux $\begin{array}{ccccc} \psi & : & Z & \to & Z/pZ \\ & & n & \mapsto & \bar{n} \end{array}$ est surjectif. De plus, $l \equiv l'\ [p^n]$ alors $l \equiv l'\ [p]$. Donc $\begin{array}{ccccc} \phi & : & Z/p^nZ & \to & Z/pZ \\ & & n & \mapsto & \bar{n} \end{array}$ est un morphisme d'anneau surjectif induit par ψ. On a montré que Z/pZ^* est cyclique, on introduit $\bar{c}$ un générateur de Z/pZ^*. On note $\bar{c_n}$ sa classe dans Z/p^nZ. $\bar{c}$ est générateur de Z/pZ^* donc c et p sont premiers entre eux donc c et p^n aussi. $\bar{c_n}$ est inversible. On pose $\bar{b} = \bar{c_n}^{p^{n-1}}$ et $u = ord(\bar{b})$.
$\bar{b}^u = \overline{1_{Z/p^nZ}}$ donc $\phi(\bar{b})^u = \overline{1_{Z/pZ}} = \bar{c}^{p^{n-1}u}$, un élément d'ordre $p-1$ car $p^{n-1} \wedge p-1 = 1$ donc $u = p-1$. $\bar{b}$ est d'ordre $p-1$.

Ainsi, le lemme 1 assure que $\bar{(}1+p)\bar{b}$ est d'ordre $p^{n-1}(p-1)$. Z/p^nZ^* est donc cyclique. □

Lemme 5. *Dans un groupe cyclique G, le nombre de solutions de l'équation* $g^n = 1$ *est de cardinal* $pgcd(\#G, n)$.

Démonstration. Pour d diviseur de m, $f(d)$ est le nombre d'éléments de G d'ordre d. Le lemme 3 affirme que $f(d) = \varphi(d)$ □

Théorème de Rabin. Soit n un entier impair.
n = $\prod_{p|n, p\in P} p^{v_p}$ et $n-1 = 2^\alpha m$ avec m impair. Pour p diviseur premier de n, $p-1 = 2^{\alpha_p} m_p$ avec m_p impair. On note finalement $\beta = \min\{\alpha_p \text{ tel que } p \mid n\}$.
On introduit 3 ensembles : $A_+ = \{x \in Z/nZ^* \text{ tel que } x^{2^{\beta-1}m} = 1\}$, $A_- = \{x \in Z/nZ^* \text{ tel que } x^{2^{\beta-1}m} = -1\}$ et $A = A_+ \cup A_-$.
On montre que $S \subset A$.

Il faut déterminer le cardinal de A. Le théorème des restes chinois donnent $Z/nZ^* \simeq \prod_{p|n} Z/p^{v_p}Z^*$. Dénombrer A_+ revient à compter le nombre de solutions de l'équation (E) : $x^{2^{\beta-1}m} \equiv 1\ [p^{v_p}]$ pour tout p diviseur premier de n. Le lemme 4 affirme que $Z/p^{v_p}Z^*$ est cyclique puis le lemme 5 donne le nombre de solutions de (E). Donc $\#(A_+) = \prod_{p|n} \text{pgcd}(2^{\beta-1}m, p^{v_p-1}(p-1)) = \prod_{p|n} 2^{\beta-1}$ pgcd$(m, p-1)$.
$A_- = \{x \in Z/nZ^* \text{ tel que } x^{2^\beta m} = 1\} \setminus \{x \in Z/nZ^* \text{ tel que } x^{2^{\beta-1}m} = 1\}$.
Donc $\#(A_-) = \prod_{p|n} 2^{\beta-1}$ pgcd$(m, p-1)$ et $\#(A) = 2\prod_{p|n} 2^{\beta-1}$ pgcd$(m, p-1)$.
Il faut minorer $\frac{\#(A)}{\varphi(n)} = 2\prod_{p|n} \frac{2^{\beta-1}\ pgcd(m,p-1)}{p^{v_p-1}\ (p-1)}$. Or pour tout p premier impair $\frac{p^{v_p-1}\ (p-1)}{2^{\beta-1}\ pgcd(m,p-1)} = \frac{p^{v_p-1}\ 2^{\alpha_p}\ m_p}{2^{\beta-1}\ pgcd(m,m_p)} \geq 2\ \frac{2^{\alpha_p}}{2^\beta} \geq 2$.
Si n est composé d'au moins 3 nombres premiers alors $\frac{\#(A)}{\varphi(n)} \leq \frac{1}{4}$.
Si n est composé de deux nombres premiers$p$ et q dont au moins un,par exemple p, vérifie $v_p \geq 2$ alors comme p est impair, $\frac{p^{v_p-1}\ 2^{\alpha_p}\ m_p}{2^{\beta-1}\ pgcd(m,m_p)} \geq 6$ et $\frac{q^{v_q-1}\ 2^{\alpha_q}\ m_q}{2^{\beta-1}\ pgcd(m,m_q)} \geq 2$ donc $\frac{\#(A)}{\varphi(n)} \leq \frac{1}{4}$.
Si $n = pq$ alors $\frac{\#(A)}{\varphi(n)} \leq \frac{1}{4}$ sauf si $\frac{(p-1)}{2^{\beta-1}\ pgcd(m,p-1)} = \frac{(q-1)}{2^{\beta-1}\ pgcd(m,q-1)} = 2$. On en déduit $\beta = \alpha_p = \alpha_q$, $m_p = \text{pgcd}(p-1, m)$ et $m_q = \text{pgcd}(q-1, m)$. Donc $m_p \mid m$ et $m_p \mid p-1$. Donc $2^\beta m_q = q-1 \equiv pq-1 \equiv n-1 \equiv 2^\alpha m \equiv 0\ [m_p]$. Donc $m_p \mid m_q$. Par symétrie, $m_q \mid m_p$ donc $m_p = m_q$. Ainsi, $p = q$, ce qui est absurde.
Si $n = p^{v_p}$ avec $v_p \geq 2$ alors $\frac{\#(A)}{\varphi(n)} \leq \frac{1}{4}$ est toujours facilement vérifié.

□

Remarque :

1. Après k itérations du test de Miller-Rabin, la probabilité, que l'algorithme renvoie qu'un nombre est premier alors qu'il ne l'est pas, est majoré par $\frac{1}{4^k}$. Le test de Miller-Rabin est très fiable, sans avoir besoin de beaucoup d'itérations.
2. La majoration est dans la plupart des cas bien meilleure. En reprenant la démonstration du théorème de Rabin on sait que $\frac{\#(S_n)}{\varphi(n)} \leq 2 \prod_{p|n} \frac{2^{\beta-1}\ pgcd(m,p-1)}{p^{v_p-1}\ (p-1)}$.
   Or on a pour tout p premier impair $\frac{p^{v_p-1}\ (p-1)}{2^{\beta-1}\ pgcd(m,p-1)} = \frac{p^{v_p-1}\ 2^{\alpha_p}\ m_p}{2^{\beta-1}\ pgcd(m,m_p)} \geq 2\ \frac{2^{\alpha_p}}{2^{\beta}} \geq 2$.
   On note t le nombre de facteurs premiers qui composent n. Avec la majoration précédente, $\frac{\#(S_n)}{\varphi(n)} \leq \frac{1}{2^{t-1}}$. Dans la plupart des cas, la proportion de faux-témoins est assez faible.
3. Il n'existe pas de nombres $n \in N$ tel que $\frac{\#(S_n)}{\varphi(n)} = \frac{1}{4}$ En effet en se servant de la démonstration on se rend compte que les seuls nombres tel que $\frac{\#(S_n)}{\varphi(n)} = \frac{1}{4}$ sont les $n = pq$ avec p et q premiers et différents. Or supposer cela mène à une contradiction qui est $p = q$.

Conjecture : On note $S_n = \{x \in Z/nZ^* \text{ tel que } x^m \equiv 1\ [p] \text{ ou } \exists\ j \in [|0, \alpha-1|] \text{ tel que } x^{2^j m} \equiv -1\ [p]\}$
$\forall \varepsilon > 0, \exists n \in N, 1/4 - \varepsilon \leq \#S_n < 1/4$.

Un programme permet d'obtenir les nombres dont la proportion de faux-témoins est maximale : $703, 1891, 12403, 38503, 79003, 88831$

Pour ces nombres la proportion de faux témoins est : $0.2307, 0.2380, 0.2452, 0.2473, 0.2481$ et 0.2482. On se rend compte que la proportion de faux témoins maximale tend vers $\frac{1}{4}$.

Un algorithme montre que ces nombres sont de la forme : $n = pq$ tels que p et q soient premiers et de la forme $2a + 1$ et $4a + 1$ avec a impair.

4 Test de primalité de Solovay-Strassen

Le test de Solovay-Srassen se sert d'un résultat, qui est lui aussi une amélioration du petit théorème de Fermat.

Définition 1. *Si p est un nombre premier et a un entier, on définit le symbole de Legendre, noté* $(\frac{a}{p})$ *par :*
0 si a est divisible par p
1 si a n'est pas divisible par p et si a est un résidu quadratique modulo p
-1 si a n'est pas un résidu quadratique modulo p

Explication du test Le test de Solovay-Strassen se base sur le critère d'Euler. Pour $n \in N$ dont on veut savoir s'il est premier ou non, on se donne $a \in Z$: si $(\frac{a}{n}) = \prod_{i=1}^{n} (\frac{a}{p_i})^{\alpha_i}$ n'est pas vérifié alors n n'est pas premier. Sinon on ne peut pas conclure, n est probablement premier. On peut itérer le test le nombre de fois le test, ce qui augmente la probabilité que n soit premier si on ne trouve pas de a tel que $(\frac{a}{n}) = \prod_{i=1}^{n} (\frac{a}{p_i})^{\alpha_i}$ ne soit pas vérifié. La complexité de l'algorithme associé au test est en $O(log(n)^3)$

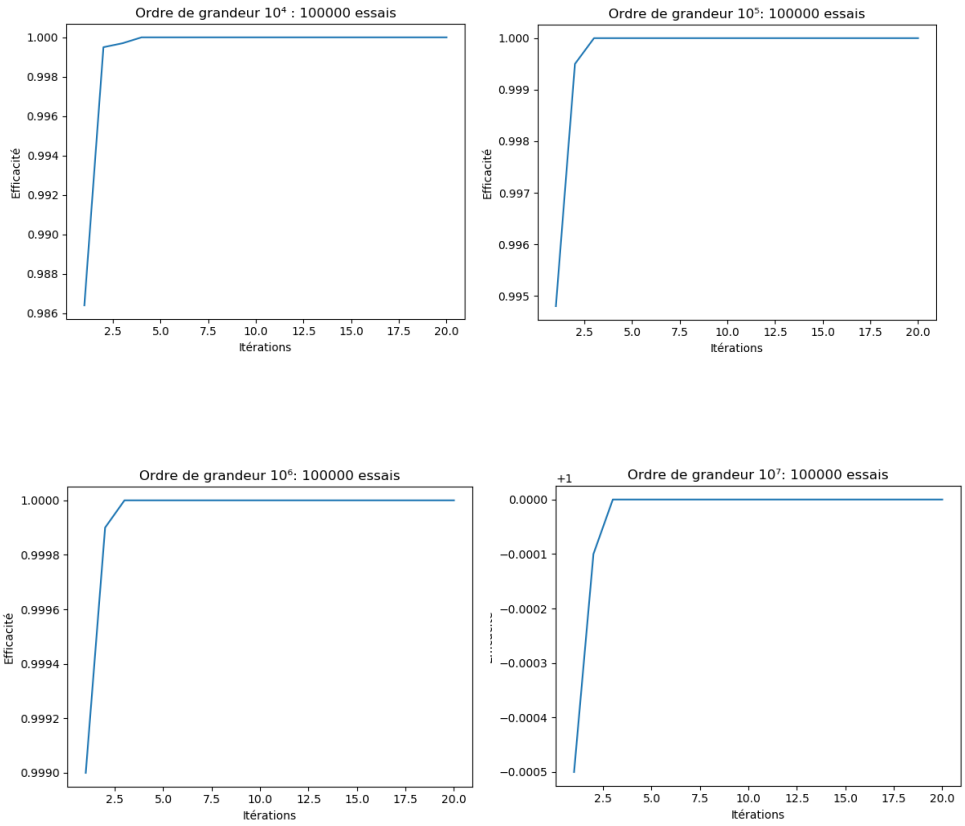

FIGURE 3 – 3 images side by side, OMG

Propriété 2 (Critère d'Euler)**.** *Soit p un nombre premier impair et $\forall a \in Z$:*
$a^{\frac{p-1}{2}} \equiv (\frac{a}{p})\ [p]$

Propriété 3. *Si $a \equiv b\ [p]$ alors $(\frac{a}{p}) = (\frac{b}{p})$*

Propriété 4. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

Propriété 5 (Loi de réciprocité quadratique)**.** $(\frac{p}{q}) = (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{q}{p})$

Généralisation : On peut généraliser le symbole de Legendre au symbole de Jacobi : Soit n un entier et $n = \prod_{i=1}^{n} p_i^{\alpha_i}$, sa décomposition en nombre premiers. Pour a un entier : $(\frac{a}{n}) = \prod_{i=1}^{n} (\frac{a}{p_i})^{\alpha_i}$

Proportion de faux témoins Un programme informatique permet de trouver des nombres dont la proportion de faux-témoins est maximale. On remarque que pour les nombres :$703, 1729, 15841, 46657$, la proportion de faux-témoins est, respectivement, $0.230, 0.375, 0.409$ et 0.444

La proportion maximale de faux témoins dépasse celle de Miller-Rabin, qui est de $\frac{1}{4}$.

Théorème 3. *Soit n un entier composé impair et $n > 9$. On note $\mathcal{S} = \{x \in Z/nZ^* \text{ tel que } a^{\frac{n-1}{2}} \equiv (\frac{a}{n}) \ [n]\}$.*
Alors $\frac{1}{4} < \frac{\#\mathcal{S}}{\varphi(n)} \leq \frac{1}{2}$

Démonstration. La démonstration est similaire à celle du théorème de Rabin. □

Références

[1] Wikipédia *Test de primalité de Miller-Rabin et Solovay-Strassen :* `https://fr.wikipedia.org/wiki/Test_de_primalité_de_Miller-Rabin`

[2] M. Wigneron : Cours anneaux `https://thiersmpe2.jimdofree.com/mathématiques/algèbre/`.

[3] J.-M. Couveignes : Quelques tests de primalité `https://www.math.u-bordeaux.fr/ jcouveig/cours/grenoble1.pdf`

[4] A. Troesch : Mars 2020 : Devoir Maison qui étudie la loi de réciprocité quadratique `http://alain.troesch.free.fr/2019/Fichiers/dm16.pdf`

[5] E. Hallouin : Quelques tests de primalité : `https://www.math.univ-toulouse.fr/ hallouin/Documents/Primalite.pdf`

[6] Université Lyon 1 : Questions d'arithmétique `http://math.univ-lyon1.fr/capes/IMG/pdf/capes7.pdf`

[7] Rutger Noot : Université de Strasbourg et CNRS : Test de primalité théorie et pratique `http://irma.math.unistra.fr/ noot/publications/primalite_irem_2011.pdf`