Test de primalité de Miller - Rabin

Lemme (Miller - Rabin): Soit $N = 1 + 2^s M$ un entier impair, avec M impair.
Si N est premier et $a \wedge N = 1$, alors ou bien $a^M \equiv 1 \ (N)$, ou bien il existe $r \in [\![0, s-1]\!]$ tel que $a^{2^r M} \equiv -1 \ (N)$.

Démonstration: On suppose N premier. Soit $a \in (\mathbb{Z}/N\mathbb{Z})^*$. Par Lagrange, l'ordre de a divise $N - 1 = 2^s M$, donc est de la forme $2^t M'$, avec $t \in [\![0, s]\!]$ et $M' \mid M$.
Si $t = 0$, on a $a^{M'} = 1$, donc $a^M = 1$. Si $t \geq 1$, on a $\left(a^{2^{t-1} M'}\right)^2 = 1$ et $a^{2^{t-1} M'} \neq 1$, donc $a^{2^{t-1} M'} = -1$ (car N est premier), donc $a^{2^{t-1} M} = -1$.

Définition: On pose $G_0 = (\mathbb{Z}/N\mathbb{Z})^*$

$S = \{ a \in G_0 \ / \ a^M = 1$ ou il existe $r \in [\![0, s-1]\!]$ tel que $a^{2^r M} = -1 \}$

Pour $A, B \in \mathbb{N}^*$, on pose $\Phi(A, B) = |\{ a \in (\mathbb{Z}/A\mathbb{Z})^* \ / \ a^B = 1 \}|$.

Lemme: Soient $t \geq 0$, $N = 1 + 2^s M = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (avec M impair).
Pour tout $i \in [\![1, k]\!]$, on pose $p_i = 1 + 2^{s_i} M_i$, $s'_i = \min(t, s_i)$, et $t_i = M \wedge M_i$.
Alors $\Phi(N, 2^t M) = 2^{s'_1 + \dots + s'_k} t_1 \dots t_k$. De plus, le cardinal de $\{ a \in G_0 \ / \ a^{2^t M} = -1 \}$ est nul si $t \geq \min_i s_i$, et égal à $\Phi(N, 2^t M) = 2^{tk} t_1 \dots t_k$ si $t < \min_i s_i$.

Démonstration: Par théorème chinois, on a $a^{2^t M} = 1$ dans $\mathbb{Z}/N\mathbb{Z}$ si et seulement si, pour tout $j \in [\![1, k]\!]$, on a $a^{2^t M} = 1$ dans $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$.
Le groupe $(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^*$ étant cyclique d'ordre $p_j^{\alpha_j - 1}(p_j - 1)$, le nombre de solutions de cette dernière équation est $\operatorname{pgcd}(2^t M, (p_j - 1) p_j^{\alpha_j - 1}) = \operatorname{pgcd}(2^t M, 2^{s_j} M_j) = 2^{s'_j} t_j$.
En effet, si $a \in (\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^*$ vérifie $a^{2^t M} = 1$, l'ordre de a divise $2^t M$ et $(p_j - 1) p_j^{\alpha_j - 1}$, donc $\operatorname{pgcd}(2^t M, (p_j - 1) p_j^{\alpha_j - 1})$. Réciproquement, si a est d'ordre divisant

$\gcd(2^t M, (p_j-1)p_j^{\alpha_j-1})$, on a $a^{2^t M}=1$. On remarque enfin que ces éléments sont au nombre de $\gcd(2^t M,(p_j-1)p_j^{\alpha_j-1})$.

On obtient donc, toujours par théorème chinois, $\Phi(N,2^t M)=2^{s_1+\dots+s_k}t_1\dots t_k$.

Pour le deuxième point, on remarque que si l'ensemble $\{a\in G_0 / a^{2^t M}=-1\}$ est non vide, il est en bijection avec $\{b\in G_0 / b^{2^t M}=1\}$. En effet, si $a\in G_0$ vérifie $a^{2^t M}=-1$, l'application

$$\begin{aligned}\{y\in G_0 / y^{2^t M}=-1\} &\longrightarrow \{b\in G_0 / b^{2^t M}=1\}\\ y &\longmapsto ay\end{aligned}$$

est bijective. On va montrer qu'un tel a existe si et seulement si 2^{t+1} divise $(p_j-1)p_j^{\alpha_j-1}$.

• $\Rightarrow$: Soit $a\in G_0$ tel que $a^{2^t M}=-1$. L'ordre de a divise $2^{t+1}M$, mais ne divise pas $2^t M$, donc vérifie une relation du type $2^{t+1}M=(2n+1)o(a)$, où $o(a)$ est l'ordre de a et $n\in\mathbb{N}$. Ceci donne $2^{t+1}\mid o(a)$ par théorème de Gauss, donc $2^{t+1}\mid p_j^{\alpha_j-1}(p_j-1)$ car $o(a)\mid p_j^{\alpha_j-1}(p_j-1)$ par Lagrange.

• $\Leftarrow$: on suppose que 2^{t+1} divise $(p_j-1)p_j^{\alpha_j-1}$. Le groupe $(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^\times$ étant cyclique, on fixe $a\in(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^\times$ d'ordre 2^{t+1}. On note encore $a\in\mathbb{Z}$ un représentant de la classe de a modulo $p_j^{\alpha_j}$. Alors $p_j^{\alpha_j}$ divise $a^{2^{t+1}}-1=(a^{2^t}-1)(a^{2^t}+1)$, mais $p_j^{\alpha_j}$ ne divise pas $a^{2^t}-1$, donc p_j divise $a^{2^t}+1$. Comme $p_j\geq 3$, on ne peut pas avoir $p_j\mid a^{2^t}-1$ et $p_j\mid a^{2^t}+1$, donc $p_j^{\alpha_j}$ divise $a^{2^t}+1$ par Gauss.

Dans $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$, on a donc $a^{2^t}=-1$, d'où $a^{2^t M}=-1$.

Finalement : $\{a\in(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^\times / a^{2^t M}=-1\}\neq\emptyset \Leftrightarrow 2^{t+1}$ divise $(p_j-1)p_j^{\alpha_j-1}=2^{s_j}M_j p_j^{\alpha_j-1}$

$$\Leftrightarrow\quad t+1\leq s_j$$

ce qui achève la preuve du lemme.

Théorème : Soit N un entier impair composé. Si $N \neq 9$, on a $\frac{|S|}{|G_0|} \leq \frac{1}{4}$.

Démonstration : Quitte à permuter les p_i, on suppose que $s_1 \leq s_2 \leq \dots \leq s_k$.

On pose $S_0 = \{a \in G_0 / a^H = 1\}$ et, pour tout $j \in [\![0, s_1 - 1]\!]$, $T_j = \{a \in G_0 / a^{2^j H} = -1\}$.

On a $S = S_0 \cup \left(\bigsqcup_{j=0}^{s_1-1} T_j \right)$, ce qui donne, en appliquant le lemme précédent à chaque morceau :

$$|S| = t_1 \dots t_k \left(1 + \sum_{j=0}^{s_1-1} 2^{jk} \right)$$

$$= t_1 \dots t_k \left(\frac{2^{ks_1} + 2^k - 2}{2^k - 1} \right)$$

d'où $$\frac{|S|}{|G_0|} = \frac{t_1 \dots t_k}{M_1 \dots M_k} \cdot \frac{1}{p_1^{\alpha_1 - 1} \dots p_k^{\alpha_k - 1}} \cdot 2^{-(s_1 + \dots + s_k)} \left(\frac{2^{ks_1} + 2^k - 2}{2^k - 1} \right).$$

- Si $k = 1$, on a $\frac{|S|}{|G_0|} = \frac{t_1}{M_1} \cdot \frac{1}{p_1^{\alpha_1 - 1}} 2^{-s_1} \cdot \frac{2^{s_1}}{2 \cdot 1} \leq \frac{1}{p_1^{\alpha_1 - 1}} \leq \frac{1}{5}$

sauf si $p_1 = 3$ et $\alpha_1 = 2$, i.e $N = 9$, auquel cas $\frac{|S|}{|G_0|} = \frac{1}{3}$.

- Si $k \geq 2$, on commence par remarquer que l'on a :

$$2^{-(s_1 + \dots + s_k)} \cdot \frac{2^{ks_1} + 2^k - 2}{2^k - 1} \leq 2^{-ks_1} \cdot \frac{2^k - 2}{2^k - 1} + \frac{1}{2^k - 1} \leq 2^{1-k},$$

donc $\frac{|S|}{|G_0|} \leq \frac{1}{8}$ si $k \geq 4$. Il reste à traiter $k = 2$.

$\frac{1}{4}$ si $k = 3$

Si l'un des α_i vaut au moins 2, on a $\frac{|S|}{|G_0|} \leq \frac{1}{p_i} \cdot \frac{1}{2} \leq \frac{1}{6}$.

On suppose donc $\alpha_1 = \alpha_2 = 1$. Si l'un des M_i est distinct de t_i, on a $\frac{|S|}{|G_0|} < \frac{t_i}{M_i} \cdot \frac{1}{2} \leq \frac{1}{6}$ car $t_i | M_i$ et $\frac{M_i}{t_i}$ est impair.

Enfin, si $M_1 = t_1$ (i.e $M_1 \mid M$) et $M_2 = t_2$ (i.e $M_2 \mid M$),

on a $P_1 P_2 = (1 + 2^{s_1} M_1)(1 + 2^{s_2} M_2) = 1 + 2^{s_1} M_1 + 2^{s_2} M_2 + 2^{s_1+s_2} M_1 M_2$

$$\| \qquad N \quad = \quad 1 + 2^{s} M$$

donc $2^s M = 2^{s_1} M_1 + 2^{s_2} M_2 + 2^{s_1+s_2} M_1 M_2$, d'où $M_1 \mid M_2$ par Gauss,

et $M_2 \mid M_1$, donc $M_1 = M_2$. Comme $P_1 \neq P_2$, on a alors $s_1 < s_2$,

a qui donne $2^{-s_1-s_2} \cdot \dfrac{2^{2s_1} + 2}{3} \leqslant 2^{s_1-s_2} \cdot \dfrac{1 + 2^{1-2s_1}}{3}$

$$\text{i.e.} \quad \frac{1 + 2^{1-2s_1}}{3} \leqslant \frac{1}{4}$$

Ceci achève la preuve du théorème.