Université Denis Diderot - Paris 7

Projet Maths-info

Tests de primalité

Benlarbi Samy
Bal dit Sollier Louis

Sous la supervision de :
Mme. Mireille Fouquet

Semestre 2 - Double licence mathématiques-informatique

Remerciements :

Nous tenons à remercier Mme Fouquet pour son accompagnement, sa disponibilité et ses conseils tout au long de la réalisation de notre projet.

Sommaire

1 Complexités :

1.1 Addition

Soient a et b deux nombres en base 2. On considère leur addition $(a + b)$, a étant le plus grand des 2. La décomposition de a en base 2 est $a = 2^k + \lambda_{k-1}2^{k-1} + ... + \lambda_0 2^0$ avec $\lambda \in \{0, 1\}$ et k tel que

$$2^k \leq a < 2^{k+1}$$

Donc on a :

$$e^{kln(2)} \leq a$$
$$ln(e^{kln(2)}) \leq ln(a)$$
$$kln(2) \leq ln(a)$$
$$k \leq \frac{ln(a)}{ln(2)}$$
$$k \leq log(a)$$

k est en fait la taille de a. Or dans l'addition $(a + b)$, il y a au pire k opérations, soit $log(a)$ opérations
Exemple : On prend $a = 110101$ et $b = 11011$. Donc $k = 6$.

$$\begin{array}{rr} & 110101 \\ + & 11011 \\ \hline & 1010000 \end{array}$$

Nous avons bien ici 6 opérations
La complexité de l'addition est bien en $O(log(a))$

1.2 Soustraction

En reprenant pour exemple les 2 nombres a et b, avec les mêmes hypothèses que précédemment, on remarque que la soustraction coûte elle aussi k opérations :

$$\begin{array}{rr} & 110101 \\ - & 11011 \\ \hline & 011010 \end{array}$$

On a effectué ici $k = 6$ opérations.
Donc la complexité de la soustraction est en $O(log(a))$

1.3 Multiplication

Prenons de nouveau a et b deux nombres en base 2. On considère cette fois-ci leur multiplication $(a \times b)$ a étant toujours le plus grand des 2. On prend $a = 10111$ et $b = 1011$. Soient k la taille de a et l la taille de b.
Rappelons que dans le pire des cas $k = log(a)$ et $l = log(b)$. Ici, nous avons donc $k = 5$ et $l = 4$.

$$\begin{array}{rr} & 10111 \\ \times & 1011 \\ \hline & 10111 \\ & 101110 \\ & 10111000 \\ \hline & 11111101 \end{array}$$

On voit ici qu'il y a autant de rang d'addition que de '1' dans b. Dans chaque rang, si on néglige les 0 ajoutés, on note que chaque addition se fait sur $k = 5$ opérations.
Dans le pire des cas, le nombre b ne sera composé que de '1' et donc la multiplication sera $l = log(b)$ fois une addition de $k = log(a)$ opérations. Donc la complexité de la multiplication de $(a \times b)$ est en $O(log(a) \times log(b))$

1.4 Complexité de la division euclidienne dans $\mathbb{Z}$

On prend cette fois-ci $a = 100110$ et $b = 110$. D'après les points développés précédemment, on sait que la complexité de la soustraction est en $O(log(a))$. Donc il ne reste plus qu'à déterminer le nombre de soustraction dont une division d'un entier de taille $k = log(a)$ par un entier de taille $l = log(b)$ aura besoin.

$$\begin{array}{r|l} 100110 & 110 \\ \cline{2-2} -110 & 110 \\ \cline{1-1} 0111 & \\ -110 & \\ \cline{1-1} 10 & \end{array}$$

Ici, avec $k = 6$ et $l = 4$ nous avons effectué 2 soustractions avant d'avoir un reste inférieur à b.
En fait, le nombre de soustractions dans une telle division est $k - l = log(a) - log(b)$ (on a bien dans l'exemple $6 - 4 = 2$ soustractions). Donc finalement, la complexité de la division est en $O(log(a)(log(a) - log(b)))$

1.5 Complexité : $b^\alpha \ mod \ n$

Soient b, α, n des entiers avec $b < n$. On va utiliser l'exponentiation modulaire pour trouver la complexité de $b^\alpha mod \ n$. En base 2, $\alpha = \alpha_0 + 2\alpha_1 + ... + 2^{k-1}\alpha_{k-1}$. Dans l'algorithme suivant, toute multiplication sera immédiatement réduite avec $mod \ n$. Ainsi, nous ne rencontrerons pas d'entiers supérieurs à n^2. On note a le produit partiel. Lorsqu'on aura terminé toutes nos opérations, a sera égal au dernier reste non-négatif de $b^\alpha \ mod \ n$.

Algorithme Commençons avec $a = 1$
Si $\alpha_0 = 1$ alors, a prend la valeur de b
Sinon, on garde $a = 1$
$b_1 = b^2 \ mod \ n$: Si $\alpha_1 = 1$ alors $a = (a \times b_1) \ mod \ n$. Sinon a
$b_2 = b_1^2 \ mod \ n$: Si $\alpha_2 = 1$ alors $a = (a \times b_2) \ mod \ n$. Sinon a
.....
$b_j = b_{j-1}^2 \ mod \ n$: Si $\alpha_{j-1} = 1$ alors $a = (a \times b_j) \ mod \ n$. Sinon a
Et $b_j = b^{2^j} \ mod \ n$
Finalement : $b_{k-1} = b^{2^{k-1}} \ mod \ n$ ce qui revient à écrire que $a = b^\alpha \ mod \ n$

A chaque étape, il y a 1 ou 2 multiplications et 1 réduction de nombres qui sont inférieurs à n^2. Donc la complexité d'une étape est en $O(log^2(n^2)) = log^2(n)$. Or il y a $k - 1 = log(\alpha)$ étapes. Donc finalement, on peut estimer la complexité de $b^\alpha mod \ m$ en $O(log(\alpha)log^2(n))$

1.6 Complexité de l'Algorithme d'Euclide :

Soient a et b deux entiers positifs avec $a > b$;
Soit r le reste de la division euclidienne de a par b;
Si $b = 0$ alors retourner a et terminer;
Tant que $b \neq 0$ faire :
Faire $r \leftarrow a \ mod \ b$, $a \leftarrow b$, $b \leftarrow r$;
Retourner a et terminer;

Il y a $O(log(a))$ divisions euclidiennes dans cet algorithme. Donc on a une complexité de $O(log(a)^2)$ en prenant en compte le fait que le produit des quotients dans les divisions euclidiennes successives est plus petit que a.

2 Test de Primalité : Théorème de Fermat

Proposition : Il existe une infinité de nombres premiers

Démonstration : Supposons qu'il existe un nombre fini de nombres premiers $p_1, p_2...., p_n$
On pose $N = (p_1 \times p_2 \times ... \times p_n) + 1$
Or tout entier naturel est divisible par au moins un nombre premier. Donc il existe k tel que p_k divise N
Or, p_k divise aussi $p_1 \times p_2 \times ... \times p_n$. Donc p_k divise $N - p_1 \times p2 \times ... \times p_n = 1$
Absurde. Donc il existe bien un infinité de nombre premiers.

2.1 "Petit" Théorème de Fermat

Théorème : Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p. Autrement dit, sous les mêmes conditions sur a et p : $a^{p-1} - 1 \equiv 0\,[p]$.

Démonstration 1
Soit p premier et pour tout $0 \leq k \leq p-1$:

$$\binom{p}{k} \equiv 0\ [p] \quad (*)$$

Or $\binom{p}{k} = \frac{p!}{k!(p-k)!} = p(p-1)...(p-k+1) \times \frac{1}{k!}$
Donc p divise $k!\binom{p}{k}$. Or p est premier, donc il l'est avec tout entier inférieur à $p-1$, et donc avec $k!$
D'après le lemme de Gauss, on a donc p divise $\binom{p}{k}$

Maintenant, montrons par récurrence que :

$$\forall a \in \mathbb{N},\ P(a) : a^p \equiv a\ [p]$$

On a que : $a^p \equiv a\ [p] \iff a^p - a \equiv 0\ [p]$

Initialisation : $a = 0$

$$0^p - 0 = 0 \equiv 0\ [p]$$

Vrai
Hérédité : Supposons la propriété $P(a)$ vraie pour un $a \in \mathbb{N}^*$. Montrons qu'elle est vraie pour $a+1$:

$$(a+1)^p - (a+1) = \sum_{k=0}^{p} \binom{p}{k} a^k - (a+1)$$

$$(a+1)^p - (a+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k + a^p - a$$

Or d'après $(*)$, p divise $\binom{p}{k}$ mais aussi $\binom{p}{k}a^k$ et donc $\sum_{k=1}^{p-1} \binom{p}{k} a^k$

Et d'après notre hypothèse de récurrence, $a^p - a \equiv 0\ [p]$. Donc $(a+1)^p - (a+1) \equiv 0\ [p]$
Par le principe de récurrence, on a donc la propriété $P(a)$ vraie pour tout $a \in \mathbb{N}^*$

Démonstration 2
Soit p premier. On considère l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ p est premier alors tout entier non multiple de p est premier avec p. Autrement dit, tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible
Donc $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps.

Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$. On sait que $Card((\mathbb{Z}/p\mathbb{Z})^*) = p-1$ car $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps et son cardinal est égal à p. D'après le théorème de Lagrange, on sait que

$$a^{p-1} \equiv 1 \ mod \ p$$

et donc

$$a^p \equiv a \ mod \ p$$

La complexité de $a^{n-1} \equiv 1 \ [p]$ est en $O(log^2(n))$ en décomposant a en puissance de 2

On peut alors se demander s'il est possible de construire un premier test de primalité se servant du théorème de Fermat comme moyen de vérification de la primalité d'un nombre. On va voir ci-dessous qu'il existe des nombres qui vérifient le "test" de Fermat mais qui ne sont pas premiers.

2.2 Nombres de Carmichaël

Certains n composés vérifie, pour des a, $a^{n-1} \equiv 1 \ [n]$ on dit alors qu'ils sont pseudo-premiers dans ces différentes bases a. Lorsque cela l'est pour toutes bases a telles que a est premier avec n, c'est alors un "nombre de Carmichaël".

Défintion : Nombre de Carmichaël
Soit $n \in \mathbb{Z}$ composé. Si $\forall a \in \mathbb{Z}$ tel que $pgcd(a, n) = 1$, on a $a^{n-1} \equiv 1 \ mod \ n$,
alors n est un nombre de Carmichaël

Remarque :
561 est le plus petit nombre de Carmichaël et 341 le plus petit pseudo- premier, le suivant étant 561.

Propriétés sur les pseudos-premiers :

1. Soit n un nombre pseudo-premier pour un $a \in \mathbb{Z}$ alors n est aussi un pseudo-premier pour a^{-1}
2. Soit n un nombre qui est pseudo-premier pour un ensemble de bases $A = \{a_1, ..., a_s\}$. Soit a une base pour laquelle n n'est pas pseudo-premier. Alors n n'est pas pseudo-premier pour les bases $= \{aa_1, ..., aa_s\}$

Preuve :

1. Soit n un pseudo-premier pour un $a \in \mathbb{Z}$
   Alors : $a^{n-1} \equiv 1 \ mod \ n$ et $(a^{n-1})^{-1} \equiv 1 \ mod \ n$
   Donc $(a^{-1})^{n-1} \equiv 1 \ mod \ n$. Ainsi n est aussi un pseudo-premier pour la base a^{-1}
2. Soit n un pseudo-premier pour un ensemble de bases $A = \{a_1, ..., a_r\}$
   $\forall i \in \{1, ..., r\}$, $a_i^{n-1} = 1 \ mod \ n$
   Soit $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv c \ mod \ n$ avec $c \neq 1$
   $\forall i \in \{1, ..., r\}$, $a^{n-1}a_i^{n-1} = c \times 1 \ mod \ n$

   Par conséquent pour l'ensemble des bases $\{aa_1, ..., aa_r\}$, n n'est plus pseudo-premier

Théorème : Il y a une infinité de nombre de Carmichaël

2.3 Probabilité

Soit n un entier qui n'est pas premier et qui n'est pas de Carmichaël. On choisit un $a \in \mathbb{Z}$ aléatoirement tel que $pgcd(a, n) = 1$

Proposition : La probabilité que n soit un nombre composé est de $\frac{1}{2}$

Démonstration : On pose $A = \{a_1, ..., a_s\}$ les bases pour lesquelles n est pseudo-premier.
Soit a une base fixé dans laquelle n n'est pas pseudo-premier. Or, d'après les propriétés précédentes, n n'est pas pseudo-premier pour les bases $\{aa_1, ..., aa_s\}$ Par conséquent, dans $(\mathbb{Z}/n\mathbb{Z})^*$, il y au moins autant de bases pour lesquelles n est pseudo-premier que de bases pour lesquelles n ne l'est pas. Alors n n'est pas pseudo-premier en base a avec une probabilité de $\frac{1}{2}$

2.4 Test de Primalité

Algorithme : Test de Fermat

Require: $k \in \mathbb{N}^*$ and $n \in \mathbb{Z}$
  for $i = 0$ to k **do**
    On choisit aléatoirement un entier a tel que $2 \leq a \leq (n-1)$
    if $a^{n-1} \neq 1$ $[n]$ **then**
      Return "n composé"
    end if
  end for
  Return "n n'est pas premier avec une probabilité de : $\frac{1}{2^k}$ "

Complexité :
On sait déjà que la complexité de a^{n-1} mod n est en $O(log(n-1)log^2(n))$. Dans le pire des cas, on aura que a est égal à $n-1$ et donc, a sera très proche de n. On peut donc écrire la complexité comme suivi : $O(log^3(n))$.
De plus on effectue k tirages d'un nombre a et à chaque passage dans la boucle, n n'est pas premier avec une probabilité de : $\frac{1}{2}$. Après k tirages on aura donc une probabilité totale de $\frac{1}{2^k}$.
On calcul donc k fois $a^{n-1} \equiv 1$ $[n]$. Ainsi la complexité du test de primalité de Fermat est en $O(k\ log^3(n))$

Cependant, comme nous l'avons vu précédemment, ce test ne marche pas pour tous les nombres (problème des nombres de Carmichaël). Nous allons donc voir un autre test, de même probabilité, mais qui fonctionne pour n'importe quelle nombre.

3 Primalité et Solovay-Strassen :

Soit $p \in \mathbb{Z}$, un nombre premier impair et soit $a \in \mathbb{Z}$ premier avec p.

3.1 Résidus Quadratiques

Définition d'un résidu quadratique : On dit que a est un résidu quadratique dans $(\mathbb{Z}/p\mathbb{Z})^*$ s'il existe $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a \equiv x^2\ mod\ p$

Proposition 1 : Le nombre de résidus quadratiques dans $(\mathbb{Z}/p\mathbb{Z})^*$ est $\frac{p-1}{2}$

Preuve :
Soit $f : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ telle que $f(x) = x^2$. Soient $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$

$$f(x \times y) = (x \times y)^2$$
$$f(x \times y) = x^2 \times y^2$$
$$f(x \times y) = f(x) \times f(y)$$

Donc f est bien un homomorphisme. On a de plus : $Ker(f) = \{x \in (\mathbb{Z}/p\mathbb{Z})^* | f(x) = 1\} = \{-1, 1\}$
Le nombre de résidus est alors le nombre d'éléments dans $Im(f)$. Or on sait que : $|(\mathbb{Z}/p\mathbb{Z})^*| = |Ker(f)| \times |Im(f)|$ et que $|Ker(f)| = 2$.
Donc :

$$2 \times |Im(f)| = |(\mathbb{Z}/p\mathbb{Z})^*|$$
$$\iff |Im(f)| = \frac{|(\mathbb{Z}/p\mathbb{Z})^*|}{2}$$
$$\iff |Im(f)| = \frac{p-1}{2}$$

Théorème (Critère d'Euler) :

- a est un résidu quadratique dans $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $a^{\frac{p-1}{2}} \equiv 1 \ mod \ p$
- a n'est pas résidu quadratique dans $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $a^{\frac{p-1}{2}} \equiv (-1) \ mod \ p$

Preuve :

- D'après le théorème de Fermat, on sait que : $a^{p-1} \equiv 1 \ mod \ p$

$$\iff a^{p-1} - 1 = 0$$

$$\iff (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = 0$$

Alors, soit p divise $(a^{\frac{p-1}{2}} + 1)$, soit p divise $(a^{\frac{p-1}{2}} - 1)$. Ce qui implique qu'on a soit $(a^{\frac{p-1}{2}} = -1)$, soit $(a^{\frac{p-1}{2}} = 1)$

- Lorsque a est un résidu, il existe x tel que $x^2 = a$ d'où :

$$(x^2)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}$$

$$x^{p-1} \ = a^{\frac{p-1}{2}}$$

Or d'après Fermat, $x^{p-1} = 1$, alors $a^{\frac{p-1}{2}} = 1$.
Considérons maintenant l'équation $y^{\frac{p-1}{2}} = 1$. Elle admet au plus $\frac{p-1}{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ car l'anneau $(\mathbb{Z}/p\mathbb{Z})^*$ est intègre. Or tous les résidus vérifient cette équation et sont au nombre de $\frac{p-1}{2}$. Les non-résidus vérifient alors forcément $a^{\frac{p-1}{2}} = -1$

3.2 Symbole de Legendre

On introduit maintenant le symbole de Legendre :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \ mod \ p \\ 1 \text{ si } a \text{ est un résidu quadratique } mod \ p \\ -1 \text{ si } a \text{ n'est pas un résidu quadratique } mod \ p \end{cases}$$

Proposition 2 : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$

Preuve :

- Si a est divisible par p, on a bien la congruence
- Sinon, d'après le critère d'Euler on a bien que $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} [p]$

Propriétés :

1. $\left(\frac{1}{p}\right) = 1$
2. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
3. Si $a \equiv b \ mod \ p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
5. Soit $m \in \mathbb{Z}$ $\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right)$

Preuve :

1. $\left(\frac{1}{p}\right) = 1^{\frac{p-1}{2}} \ mod\ p = 1$
2. D'après le critère d'Euler, on a : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \ mod\ p = \pm 1$, donc $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
3. Si $a \equiv b \ mod\ p$ alors $a^{\frac{p-1}{2}} = b^{\frac{p-1}{2}} \ mod\ p$. Or $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ et $\left(\frac{b}{p}\right) = b^{\frac{p-1}{2}}$. Donc $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} = \left(\frac{ab}{p}\right)$
5. Soit $m \in \mathbb{Z}$ Si p divise a alors on a bien $\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right) + \left(\frac{mp}{p}\right) = \left(\frac{a}{p}\right)$
   On suppose maintenant que p ne divise pas a. $\left(\frac{a+mp}{p}\right) = 1$ si et seulement si a est un résidu quadratique. C'est-à-dire si et seulement si $a + mp$ est aussi un résidu. Et donc on a : $\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right) = 1$

Proposition(admise) :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Théorème (admis) : Loi de Réciprocité Quadratique Soient p et q, deux premiers impairs.

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

Dans la pratique, on applique la loi de réciprocité quadratique, pour calculer le symbole de Legendre, sous réserve de la primalité de p. Lorsque la factorisation de a n'est pas évidente, voir difficile, le calcul du symbole de Legendre l'est aussi. On utilise le symbole de Jacobi introduit ci-dessous.

3.3 Symbole de Jacobi

Définition du Symbole de Jacobi : Soit $n \in \mathbb{Z}^*$ impair et $n = p_1^{\alpha_1} p_2^{\alpha_2} ..... p_k^{\alpha_k}$
On définit le symbole de Jacobi $\left(\frac{a}{n}\right)$ par : $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} .... \left(\frac{a}{p_k}\right)^{\alpha_k}$

Donc, lorsque n est premier, le symbole de Jacobi est le symbole de Legendre

Propriétés : Soient m, n positifs impairs et a, b entiers quelconques. Alors :

1. $\left(\frac{a}{1}\right) = 1$
2. Si n est premier alors $\left(\frac{a}{n}\right)$ est le symbole de Legendre
3. Si a et n ne sont pas premiers entre eux alors $\left(\frac{a}{n}\right) = 0$
4. Si a et n sont premiers entre eux alors $\left(\frac{a}{n}\right) = \pm 1$
5. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
6. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
7. Si $a \equiv b \ mod\ n \Longrightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

Théorème : Soit $n > 3$ un entier impair. Alors

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Preuve :

$$Soit\ \phi(n) = \begin{cases} (-1)^{\frac{n^2-1}{8}} \text{ si } n \text{ est impair} \\ 0 \text{ si } n \text{ est pair} \end{cases}$$

Montrons que $\left(\frac{2}{p}\right) = \phi(p)$

On a $p^2 \equiv 1\ mod\ 8$ pour p impair premier. $(\mathbb{Z}/p\mathbb{Z})$ contient une racine 8-ième de l'unité. Soit ϵ l'une d'entres elles. Alors $\epsilon^4 = -1$. Posons $G = \sum_{i=0}^{7} \phi(i)\epsilon^i$. On a $\epsilon^5 = \epsilon^4 \times \epsilon = -\epsilon$ et $\epsilon^7 = -\epsilon^3$
Alors

$$G = \epsilon - \epsilon^3 - \epsilon^5 + \epsilon^7$$

$$G = 2(\epsilon - \epsilon^3)$$

et

$$G^2 = 4(\epsilon^2 - 2\epsilon^4 + \epsilon^6) = 8$$

Donc

$$G^p = (G^2)^{\frac{p-1}{2}} \times G$$

$$G^p = 8^{\frac{p-1}{2}} \times G$$

$$G^p = \left(\frac{8}{p}\right) \times G$$

d'après le critère d'Euler
Et on sait que $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$. Donc $\left(\frac{8}{p}\right) \times G = \left(\frac{2}{p}\right) \times G$

Théorème (admis): Loi de Réciprocité Quadratique pour le Symbole de Jacobi :

Soient m un entier relatif et n un entier naturel impair.

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \times \frac{n-1}{2}} \left(\frac{n}{m}\right)$$

Algorithme : Calcul du Symbole de Jacobi

Require: $n \geq 3$ impair, $m \in \mathbb{Z}$ and $s = 1$
  Calculons $\left(\frac{m}{n}\right)$
  if $m < 0$ **then**
    $m \leftarrow -m$
    if $n \equiv 1\ mod\ 4$ **then** $s \leftarrow s \times (-1)$
  end if
  while $m \geq 2$ **do**
    if m est pair **then**
      $m \leftarrow \frac{m}{2}$
      if $n \equiv \pm 3\ mod\ 8$ **then** $s \leftarrow s \times (-1)$
    else
      if $n \neq 1\ mod\ 4$ **et** $m \neq 1\ mod\ 4$ **then** $s \leftarrow s \times (-1)$
      Soit r le reste de la division euclidienne de n par m
      $n \leftarrow m$
      $m \leftarrow r$
    end if
  end while
  if $m = 0$ **then**
    $s \leftarrow 0$
  end if
  Return : $s = \left(\frac{m}{n}\right)$

Complexité : $O(log^2(n))$ Cet algorithme est principalement constitué de divisions euclidiennes et au pire son nombre de divisions euclidiennes est égal à celui de l'algorithme d'Euclide et on connaît déjà la complexité de ces opérations. Donc dans le pire des cas, on aura donc une complexité en : $O(log^2(n))$.

3.4 Solovay-Strassen

Pour déterminer si un entier impair n donné est premier, on peut tester pour un grand nombre de valeurs aléatoires de a, si la congruence

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

est satisfaite. Si elle est fausse pour un certain entier a, alors on sait que n n'est pas premier. Si on essaie de savoir si un entier n est premier par le test de Fermat, nous savons que la proportion de contre-exemples est supérieure à 50% si n est composé et n'est pas un nombre de Carmichaël. Mais si n est un nombre de Carmichaël les uniques contre-exemples pour le test de Fermat sont tous les entiers a tels que $pgcd(a, n) = 1$, et leur nombre peut être très petit. Solovay et Strassen ont alors énoncé un théorème permettant d'affirmer que ce problème n'existe pas dans le cas que nous étudions ici.

Cependant, de même qu'avec le test de primalité de Fermat, il y a des nombres composés qui vérifient cette équivalence. Un entier a est appelé menteur d'Euler si l'équivalence est satisfaite alors que n est composé. Un témoin d'Euler est un a pour lequel l'égalité n'est pas satisfaite.

À la différence du test de primalité de Fermat, pour chaque entier composé n, au moins la moitié de tous les a de $(\mathbb{Z}/n\mathbb{Z})^*$ sont des témoins d'Euler. Par conséquent, il n'y a aucune valeur de n pour laquelle tous les a sont des menteurs, alors que c'est le cas pour les nombres de Carmichaël dans le test de Fermat.

Théorème : Soit n un entier positif impair et composé. Il existe un entier a tel que $pgcd(a, n) = 1$ et $a^{\frac{(n-1)}{2}} \not\equiv \left(\frac{a}{n}\right)\ mod\ n$

Preuve : Procédons par disjonction de cas: Soit n est sans carrés parfaits, soit il a un facteur premier qui se répète.

* Supposons n composé et sans carrés parfaits, alors $n = p_1 \times p_2 \times ... \times p_r$ avec $r \geq 2$, sa décomposition en produit de facteurs premiers impairs. La moitié des entiers non-nuls (mod p_1) n'étant pas des carrés, il existe alors un $b \in \mathbb{R}$ tel que $\left(\frac{b}{p_1}\right) = -1$. D'après le théorème des restes chinois, il existe a tel que :

$$a \equiv b\ mod\ p_1$$

et

$$a \equiv 1\ mod\ p_2...p_r$$

On a alors que a est premier avec tous les p_i, et donc avec n. De plus,

$$\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$$

et

$$\left(\frac{a}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$$

pour $i > 1$, alors:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)...\left(\frac{a}{p_r}\right) = \left(\frac{a}{p_1}\right) = -1.$$

Si on considère que $a^{\frac{(n-1)}{2}} \equiv \left(\frac{a}{n}\right) mod\ n$, alors $a^{\frac{(n-1)}{2}} \equiv (-1)\ mod\ n$. Or p_2 divise n, car $n = p_1 \times p_2 \times ... \times p_r$. Donc on a

$$1 \equiv (-1)\ mod\ p_2$$

Or $a \equiv 1 \ mod \ p_2$. Il y a donc contradiction car p_2 est supérieur à 2.

* Supposons cette fois-ci que n possède un facteur premier p qui se répète. Alors $n = p^k \times m$ où $k > 2$, avec p et m premiers entre eux. D'après le théorème des restes chinois, il existe un $a \in \mathbb{Z}$ qui satisfait $a \equiv (1+p) \ mod \ p^2$ et $a \equiv 1 \ mod \ m$
Donc a n'est pas divisble par p et a premier avec m, et donc a premier avec n. Si $a^{\frac{(n-1)}{2}} \equiv \left(\frac{a}{n}\right) \ mod \ n$ alors on obtient $a^{n-1} \equiv 1 \ mod \ n$. Montrons que cela est impossible.
On va utiliser p^2 comme module pour avoir $a^{n-1} \equiv 1 \ mod \ p^2$. Or $a \equiv (1+p) \ mod \ p^2$, on a $(1+p)^{n-1} \equiv 1 \ mod \ p^2$. D'après le binôme de Newton, $(1+p)^{n-1} \equiv (1+(n-1) \times p) \ mod \ p^2$, et alors, $(1+(n-1) \times p) \equiv 1 \ mod \ p^2$. En enlevant 1 des deux côtés, on obtient $((n-1) \times p) \equiv 0 \ mod \ p^2$, et donc $(n-1) \equiv 0 \ mod \ p$. Mais n est un multiple de p, il y a donc contradiction.

Dans les deux cas énoncés précédemment, on a bien démontré le théorème.

Probabilité :

Proposition : Soit $n > 1$, un entier impair. La proportion d'entiers qui sont des témoins d'Euler pour n est supérieur à 50%

Preuve : Soit $n > 1$ un entier impair composé.
Montrons que $Card(\{1 \leq a \leq n-1\}), \ pgcd(a,n) = 1$ et $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \ mod \ n\}) < \frac{n-1}{2}$
Soient $A = \{1 \leq a \leq n-1 \ , \left(\frac{a}{n}\right) = \pm 1$ et $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \ mod \ n\}$
$B = \{1 \leq a \leq n-1 \ \left(\frac{a}{n}\right) = \pm 1$ et $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \ mod \ n\}$
et $C = \{1 \leq a \leq n-1 \ \left(\frac{a}{n}\right) = 0\}$
A,B et C sont disjoints. $A \neq \emptyset$ car $1 \in A$, $C \neq \emptyset$ car n est composé et B n'est pas vide d'après le premier théorème. Montrons que $|A| < \frac{n-1}{2}$. Soit $b_0 \in B$. Montrons que $Ab_0 \subset B$
Pour tout $a \in A$, ab_0 est premier avec n par la congruence d'Euler et :

$$(ab_0)^{\frac{n-1}{2}} \equiv (a)^{\frac{n-1}{2}} \times (b_0)^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(b_0)^{\frac{n-1}{2}} \ mod \ n$$

Donc : soit $(ab_0 \ mod \ n) \subset A$, soit $(ab_0 \ mod \ n) \subset B$

$$(ab_0)^{\frac{n-1}{2}} \equiv \left(\frac{ab_0}{n}\right) = \left(\frac{a}{n}\right) \times \left(\frac{b_0}{n}\right) \ mod \ n$$

et alors on a :

$$\left(\frac{a}{n}\right) \times \left(\frac{b_0}{n}\right) \equiv \left(\frac{a}{n}\right) \times b_0^{\frac{n-1}{2}} \ mod \ n$$

Or, on a ici une contradiction avec l'appartenance de b_0 à B. Donc $(ab_0 \ mod \ n) \in B \forall a \in A$ et on a $Ab_0 \subset B$

Posons a et $a' \in A$, si $ab_0 \equiv a'b_0 \ mod \ n$ alors $a = a'$ Dans ce cas, $|Ab_0| = |A|$ et on a alors $|A| = |Ab_0| \leq |B|$ car $Ab_0 \subset B$. Cela implique donc que

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|$$

Donc $|A| \leq \frac{n-1}{2}$

Finalement le test de Solovay-Strassen permet d'avoir une probabilité de 1/2

Algorithme : Test de Solovay-Strassen

Require: $k \in \mathbb{N}^*$ and $n \geq 3$ impair
  for $i = 0$ to k **do**
    On choisit aléatoirement un entier a tel que $2 \leq a \leq (n-2)$
    $p \leftarrow (a^{\frac{n-1}{2}} \ mod \ n)$
    if $p \neq 1$ et $p \neq n-1$ **then**
      Return "n composé"
    end if
    $j \leftarrow \left(\frac{a}{n}\right)$
    if $p \neq (j \ mod \ n)$ **then**
      Return "n composé"
    end if
  end for
  Return "n composé avec une probabilité de $\frac{1}{2^k}$"

Complexité : $O(klog(n)^3)$. La probabilité pour qu'un nombre composé ne soit pas détecté est inférieure à $\frac{1}{2^k}$ après k étapes. Contrairement au test de Fermat, ce test marche pour tous les n.

4 Primalité et Miller-Rabin

Tout comme le test de Fermat et le test de Solovay-Strassen, on va ici vérifier une équivalence sur un nombre p pour savoir si p est premier.

Proposition : Dans $\mathbb{Z}/p\mathbb{Z}$, avec p premier et $p > 2$, 1 et -1 sont les seules racines de 1 mod p.

Supposons maintenant n un nombre premier impair et $n > 2$. Ainsi $n-1$ est pair et on peut donc l'écrire comme ceci : $n - 1 = 2^s \times d$ où s et d sont des entiers positifs et d est impair. On a $\forall a \in (\mathbb{Z}/p\mathbb{Z})^*$:

$$a^d \equiv 1 \ mod \ n$$

ou

$$a^{2^r \times d} \equiv -1 \ mod \ n$$

avec $0 \leq r \leq s-1$
En effet d'après le théorème de Fermat, $a^{n-1} = a^{d(2^s)} \equiv 1 \ mod \ n$ D'après la précédente proposition, en prenant de façon répétée des racines carrés à partir de a^{n-1}, nous obtiendrons soit 1 soit -1. Si on tombe sur -1 alors la première équation est vérifiée. Au contraire, si nous n'avons jamais -1, nous tomberons finalement la première équation. Le test de Miller-Rabin se base sur la contraposée de ce qui précède :

Si on peut trouver a tel que

$$a^d \neq 1 \ mod \ n$$

et

$$a^{2^r \times d} \neq -1 \ mod \ n$$

$\forall 0 \leq r \leq s-1$
Alors n est composé et donc n'est pas premier. De plus, comme pour le test de Solovay-Strassen, il existe des témoins de n pour le test de Miller-Rabin. Ce sont les éléments qui vérifient la contraposée ci-dessus.

Théorème de Rabin:
Soit n un entier impair composé avec $n > 9$ et $n - 1 = 2^s \times d$ pour d impair et $M = \{x \in \mathbb{Z}/n\mathbb{Z} | x^m = 1$ ou $x^{2^i \times m} = -1$ pour $i \in \{0, 1, 2, ..., s-1\}\}$
Alors

$$|M| \leq \frac{\phi(n)}{4}$$

Démonstration :

Ce Théorème est lié au nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre divisant $n-1$.Pour cela nous allons utiliser le fait que $(\mathbb{Z}/n\mathbb{Z})^*$ est un produit de groupes cycliques.
Notons $n = \prod_{p|n} p^{\epsilon_p}$ et pour tout p premier divisant n, on pose $p-1 = 2^{\alpha_p} \times m_p$, avec m impair.
Enfin notons $\beta = min\{\alpha_p\ , p|n\}$. Ainsi, 2^β est la plus grande puissance de 2 divisant tous les $(p-1)$ pour p diviseurs premiers de n

On a

$$N_+ = \{x \in \mathbb{Z}/n\mathbb{Z} | x^{2^{\beta-1}\times m} = 1\}$$

$$N_- = \{x \in \mathbb{Z}/n\mathbb{Z} | x^{2^{\beta-1}\times m} = -1\}$$

et $N = N_+ \cup N_-$
Montrons d'abord que $M \subset N$:
Par le théorème des restes chinois, on a:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{p|n} (\mathbb{Z}/p^{\epsilon_p}\mathbb{Z})^*$$

Or on sait que pour tout p premier, impair, et tout $\epsilon > 0$, $(\mathbb{Z}/p^\epsilon\mathbb{Z})^*$ est cyclique et $|(\mathbb{Z}/p^\epsilon\mathbb{Z})^*| = p^{\epsilon-1} \times (p-1)$
Ainsi on sait que chaque élément, du produit est un groupe cyclique de cardinal $\phi(\epsilon_p) = p^{\epsilon_p - 1} \times (p-1)$
Pour $x \in (\mathbb{Z}/n\mathbb{Z})^*$, si $x^m = 1\ mod\ n$, on voit tout de suite que $x \in N$
car

$$x^{n-1} = 1$$

$$\Leftrightarrow x^{2^\alpha \times m} = 1$$

$$\Leftrightarrow x^{2^{\beta-1}\times m} = 1$$

Si maintenant, $x^{2^i \times m} = -1$ pour $i \in 0, 1, ..., \alpha - 1$, alors $(x^m)^{2^i} = -1\ mod\ n$. Ainsi, $(x^m)^{2^i} = -1\ mod\ p^{\epsilon_p}$ pour tout premier p premier, divisant n.

En particulier cela veut dire que x^m est d'ordre 2^{i+1}, pour tout p premier divisant n. Donc $2^{i+1} | \phi(p^{\epsilon_p})$. On a alors que $i + 1 \leq \beta$ et donc $x \in N$

Dénombrons maintenant N_-, N_+, et N:
Dénombrer N_+ revient à compter les solutions de $x^{2^{\beta-1}\times m} = 1\ mod\ p^{\epsilon_p}$ pour chaque p premier divisant n. Or, on sait que dans un groupe multiplicatif cyclique H, le nombre de solutions de l'équation $y^\epsilon = 1$ est le pgcd de $|H|$ et ϵ. On a donc :

$$|N_+| = \prod_{p|n} pgcd(2^{\beta-1} \times m, p^{\epsilon_p - 1} \times (p-1))$$

$$|N_+| = \prod_{p|n} 2^{\beta-1} \times pgcd(m, (p-1))$$

Pour N_-, si on pose $A = \{x \in \mathbb{Z}/p^{\epsilon_p}\mathbb{Z} | x^{2^{\beta-1}\times m} = -1\}$ on remarque que :

$$A = \{x \in \mathbb{Z}/p^{\epsilon_p}\mathbb{Z} | x^{2^\beta \times m} = 1\}$$

et donc que

$$|A| = pgcd(2^\beta \times m, p^{\epsilon_p - 1} \times (p-1)) - pgcd(2^{\beta-1} \times m, p^{\epsilon_p - 1} \times (p-1))$$

$$|A| = 2^\beta \times pgcd(m, p-1) - 2^{\beta-1} \times pgcd(m, p-1)$$

$$|A| = 2^{\beta-1} \times pgcd(m, p-1)$$

Ainsi,

$$|N_-| = |N_+| \Rightarrow |N| = 2 \times \prod_{p|n} 2^{\beta-1} pgcd(m, p-1)$$

Pour conclure , montrons que :

$$\frac{|N|}{\phi(n)} = 2 \times \prod_{p|n} \frac{2^{\beta-1} pgcd(m, p-1)}{p^{\epsilon_p - 1} \times (p-1)} \leq \frac{1}{4}$$

Pour cela montrons que :

$$\prod_{p|n} \frac{p^{\epsilon_p - 1} \times (p-1)}{2^{\beta-1} pgcd(m, p-1)} \geq 8 \ (*)$$

Comme $\frac{(p-1)}{2^{\beta-1} \times pgcd(m,p-1)} \geq 2$, si n est divisible par au moins 3 premiers distincts alors (*) est vérifiée.
Dans le cas où n ne possède que 2 premiers dans sa décomposition, on a :
1. $\epsilon_p \geq 2$ indique clairement que $\prod_{p|n} \frac{p^{\epsilon_p - 1} \times (p-1)}{2^{\beta-1} pgcd(m,p-1)} \geq 4_p \geq 8$
2. $n = p \times q$ avec (*) non satisfaite quand :

$$\frac{(p-1)}{2^{\beta-1} pgcd(m, p-1)} = \frac{(q-1)}{2^{\beta-1} pgcd(m, q-1)} = 2$$

$$\iff \begin{cases} p - 1 = 2^{\beta} \times pgcd(p-1, m) = 2^{\alpha_p} \times m_p \\ q - 1 = 2^{\beta} \times pgcd(q-1, m) = 2^{\alpha_q} \times m_q \end{cases}$$

$$\implies \begin{cases} \alpha_p = \alpha_q = \beta \\ pgcd(p-1, m) = m_p \\ pgcd(q-1, m) = m_q \end{cases}$$

Ainsi, m_p doit diviser m et $p-1$ ce qui est impossible car

$$2^{\beta} \times m_q = q - 1$$

$$2^{\beta} \times m_q \equiv pq - 1$$

$$2^{\beta} \times m_q \equiv n - 1$$

$$2^{\beta} \times m_q \equiv 2^{\alpha} \times m$$

$$2^{\beta} \times m_q \equiv 0 \ mod \ n$$

Ce qui équivaut à dire que $m_p | m_q$. Par symétrie, on a $m_q | m_p$ et donc $m_p = m_q$ et par suite $p = q$. Or ceci est impossible.

Enfin, si n est égal à p^{ϵ_p}, et comme n est impair, composé et supérieur à 9, on a $p \geq 5$ et $\epsilon_p \geq 2$ ou $p \geq 3$ et $\epsilon_p \geq 3$. Dans les 2 cas, (*) est bien vérifiée.
Donc finalement :

$$\frac{|N|}{\phi(n)} = \prod_{p|n} \frac{2^{\beta-1} pgcd(m, p-1)}{p^{\epsilon_p - 1} \times (p-1)} \leq \frac{1}{8}$$

$$\iff \frac{|N|}{\phi(n)} \leq \frac{1}{4}$$

Donc pour un n impair composé supérieur à 2, on a au plus 3/4 des bases a qui sont des témoins de la compositions de n. Ainsi, cela nous permet de dire que la probabilité de l'échec du test de Miller-Rabin est de 1/4. On voit alors que ce test est bien meilleur que celui de Solovay-Strassen, ce dernier ayant une probabilité de 1/2.

Algorithme : Test de Miller-Rabin

Require: $k \in \mathbb{N}^*$ and $n \in \mathbb{Z}$
  for $i = 0$ to k **do**
    On choisit aléatoirement un entier a tel que $2 \leq a \leq (n-2)$
    $x \leftarrow a^d \ mod \ n$
    if $x \neq 1$ et $x \neq n-1$ **then**
      Return "n composé"
    end if
    for $j = 0$ to $s-1$ **do**
      $x \leftarrow x^2 \ mod \ n$
      if $x \neq 1$ **then**
        Return "n composé"
      end if
    end for
  end for
  Return "n composé avec une probabilité de $\frac{1}{4^k}$"

Complexité : Cet algorithme n'utilise que des divisions euclidiennes et une opération $a^d \ mod \ n$. Or on connaît déjà le coût de ces opérations. On a donc une complexité en $O(klog(n)^3)$. La probabilité pour qu'un nombre composé ne soit pas détecté est au plus $\frac{1}{4^k}$ après k tirages. Contrairement au test de Fermat, ce test marche pour tous les n.

5 Temps d'éxécution des algorithmes

Les différents algorithmes présentés ont été programmé en C, en utilisant la bibliothèque GMP pour "Gnu Multiple Precision Arithmetic Library". L'utilisation de cette dernière s'est avérée indispensable, car elle permet d'user d'entiers dont la taille augmente dynamiquement jusqu'à la précision voulue. Donc en concaténant de nombreux "mots" ensemble, la bibliothèque peut supporter jusqu'à 1024 bits, en allouant dynamiquement la mémoire pour gérer chaque bit de précision en trop quand cela est nécessaire.

Nous avons utilisé l'algorithme de Mersenne-Twister fourni par la bibliothèque GMP afin de générer des nombres aléatoirement.

Le tableau ci-dessous contient les temps d'éxécution en millisecondes de chaque algorithme pour un nombre d'itérations égal à 300. Nous avons testé plusieurs nombres :
-561 et 1436697831295441 qui sont des nombres de Carmichaël
-859394766929 et 311 qui sont des nombres premiers
-2769275 qui est un nombre composé
-9874578924857728445 qui est un nombre tapé aléatoirement et qui ne passe aucun test

Les mentions dans le tableau sont :
-(v) si le nombre passe le test
-(x) s'il est trouvé composé par l'algorithme.

Nombres	561	1436697831295441	311	859394766929	2769275	9874578924857728445
Fermat	1100 ms (v)	1676 ms (v)	2514 ms (v)	1754 ms (v)	1257 ms (x)	1362 ms (x)
Solovay-Strassen	1324 ms (x)	1601 ms (x)	2947 ms (v)	2792 ms (v)	1706 ms (x)	1806 ms (x)
Miller-Rabin	1158 ms (x)	1474 ms (x)	2644 ms (v)	2007 ms (v)	1901 ms (x)	1804 ms (x)