Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

Chapitre II - Tests et critères de primalité

On se préoccupe ici du problème de savoir si un entier donné est premier ou non. Un entier naturel qui n'est pas premier est appelé composé. Dans l'étude des cryptosystèmes à clés publiques, on a vu l'importance de pouvoir expliciter de grands nombres premiers. Il est donc nécessaire de disposer de tests et de critères de primalité performants. Un test de primalité est en fait un critère de non primalité. Étant donné un entier n, il permet de démontrer que n est composé si tel est le cas. Il suffit qu'il ne satisfasse pas une condition du test. Si n «passe» avec succès de nombreux tests, il y a une grande probabilité pour que n soit premier, mais cela n'en fournit pas la preuve. Les critères de primalité permettent d'établir que n est premier si tel est le cas. On étudiera ceux concernant les entiers n pour lesquels on connaît les diviseurs premiers de $n-1$ (critère de Lehmer), ou bien les diviseurs premiers de $n+1$ (critère de Lucas-Lehmer). On exposera par ailleurs une variante du théorème d'Agrawal, Kayal et Saxena, qui est un critère de primalité consistant, pour l'essentiel, à vérifier si une certaine congruence dans l'anneau $\big(\mathbb{Z}/n\mathbb{Z}\big)[X]$ est satisfaite.

Table des matières

1. Test de Fermat

En rapport avec son efficacité, c'est le test de primalité, i.e. le critère de composition, le plus simple. Il repose directement sur le petit théorème de Fermat.

Lemme 2.1 (Test de Fermat). *Soit $n \geq 2$ un entier. S'il existe un entier a tel que*

$$1 < a < n \quad et \quad a^{n-1} \not\equiv 1 \bmod. n, \tag{1}$$

alors n est composé.

S'il existe un entier a tel que la condition (1) soit réalisée, on dit que n échoue au test de Fermat. Parmi les entiers susceptibles de satisfaire (1), il y a évidemment ceux qui ne sont pas premiers avec n. Si l'on trouve un tel entier a, on dit que a est un témoin de non primalité de n qui est issu de la divisibilité. Pour les entiers a premiers avec n satisfaisant la condition (1), autrement dit, ceux constituant un véritable contre-exemple au petit théorème de Fermat, on utilise la terminologie suivante :

Définition 2.1. *Soit $n \geq 2$ un entier. On appelle témoin de Fermat pour n, tout entier a premier avec n, tel que $1 < a < n$ et $a^{n-1} \not\equiv 1 \bmod. n$.*

Si n est composé, il y a très souvent de nombreux témoins de Fermat pour n, mais pas toujours. En effet, il existe des entiers composés qui ne possèdent pas de témoins de Fermat. On les appelle les nombres de Carmichael. Ce sont exactement les entiers n composés qui sont sans facteurs carrés, et tels que pour tout diviseur premier p de n, l'entier $p-1$ divise $n-1$ (exercice 7 du chapitre II). L'entier 561 est le plus petit d'entre eux. Ils sont impairs et ont au moins trois diviseurs premiers. On sait par ailleurs qu'il existe une infinité de nombres de Carmichael. En fait, pour tout x assez grand, il y a au moins $x^{\frac{2}{7}}$ nombres de Carmichael plus petits que x (Alford, Granville, Pomerance, 1994). Cela étant :

Lemme 2.2. *Soit $n \geq 2$ un entier possédant un témoin de Fermat. Alors, il existe au moins $\frac{\varphi(n)}{2}$ témoins de Fermat pour n.*

Démonstration : L'ensemble des éléments $x \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ tels que $x^{n-1} = 1$ est un sous-groupe H de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. S'il existe un témoin de Fermat pour n, l'ordre de H est au plus $\frac{\varphi(n)}{2}$. Il y a donc au moins $\frac{\varphi(n)}{2}$ éléments $x \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ tels que $x^{n-1} \neq 1$, d'où l'assertion.

Pour les entiers composés qui ne sont pas des nombres de Carmichael, on constate expérimentalement que les entiers $a = 2$ ou $a = 3$ en sont souvent des témoins de Fermat. Un entier $a \geq 2$ étant donné, cela suggère l'étude des entiers composés pour lesquels a n'est pas un témoin de Fermat, d'où la définition suivante :

Définition 2.2. *Soient $n \geq 2$ un entier composé et a un entier tel que $1 < a < n$. On dit que n est pseudo-premier en base a si l'on a $a^{n-1} \equiv 1 \bmod. n$. Un entier qui est pseudo-premier en base 2 est appelé plus simplement pseudo-premier.*

Exemple 2.1. Soient p et q des nombres premiers impairs distincts. Posons

$$n = pq \quad \text{et} \quad d = \operatorname{pgcd}(p-1, q-1).$$

Soit a un entier tel que $1 < a < n$. Vérifions l'équivalence

$$n \text{ est pseudo-premier en base } a \iff a^d \equiv 1 \bmod. n. \tag{2}$$

On a l'égalité

$$n-1=(p-1)q+(q-1). \tag{3}$$

Par suite, on a

$$a^{n-1}\equiv a^{q-1} \text{ mod. } p \quad \text{et} \quad a^{n-1}\equiv a^{p-1} \text{ mod. } q.$$

Supposons n pseudo-premier en base a. D'après les congruences précédentes, on a alors

$$a^{p-1}\equiv 1 \text{ mod. } q \quad \text{et} \quad a^{q-1}\equiv 1 \text{ mod. } p.$$

Puisque l'on a $a^{p-1}\equiv 1$ mod. p et $a^{q-1}\equiv 1$ mod. q, on obtient

$$a^{p-1}\equiv 1 \text{ mod. } n \quad \text{et} \quad a^{q-1}\equiv 1 \text{ mod. } n.$$

Ainsi, n divise le pgcd de $a^{p-1}-1$ et $a^{q-1}-1$, qui n'est autre que a^d-1.
Inversement, si $a^d\equiv 1$ mod. n, on a $a^{p-1}\equiv 1$ mod. n et $a^{q-1}\equiv 1$ mod. n. L'égalité (3) entraîne alors $a^{n-1}\equiv 1$ mod. n. Cela établit (2).
Il en résulte par exemple que si $2^d\leq n$, alors 2 est un témoin de Fermat pour n.

Il est facile de déterminer le nombre de bases en lesquelles un entier n composé, disons impair, est pseudo-premier, pourvu que l'on connaisse les diviseurs premiers de n.

Lemme 2.3. *Soit n un entier naturel impair composé. Le nombre d'entiers a tels que $1<a<n$ et que n soit pseudo-premier en base a est*

$$-1+\prod_{p|n}\text{pgcd}(n-1,p-1),$$

où p parcourt l'ensemble des diviseurs premiers de n.

Démonstration : Il s'agit de dénombrer les solutions de l'équation $x^{n-1}=1$ dans le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Soit $n=p_1^{n_1}\cdots p_r^{n_r}$ la décomposition de n en facteurs premiers p_i distincts deux à deux. Compte tenu du théorème chinois, il s'agit donc de compter les solutions de cette équation dans le groupe $\left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)^*$ pour $i=1,\cdots,r$. Puisque n est impair, les p_i le sont aussi et $\left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)^*$ est cyclique. Le nombre de solutions de l'équation $x^{n-1}=1$ dans $\left(\mathbb{Z}/p_i^{n_i}\mathbb{Z}\right)^*$ est le pgcd de $n-1$ et $p_i^{n_i-1}(p_i-1)$ (exercice 3 du chapitre II), autrement dit le pgcd de $n-1$ et p_i-1. Il y a donc

$$\prod_{i=1}^{r}\text{pgcd}(n-1,p_i-1)$$

éléments $x\in\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ tels que $x^{n-1}=1$, d'où le résultat vu que l'on enlève par définition la solution $x=1$.

Pour tout $x > 0$, soit $\pi(x)$ le nombre des nombres premiers plus petits que x. Rappelons que la fonction $\pi(x)$ est équivalente à $\frac{x}{\log x}$ quand x tend vers l'infini (théorème des nombres premiers). Pour chaque entier $a \geq 2$, notons $P_a(x)$ le nombre d'entiers pseudo-premiers en base a plus petit que x. On peut démontrer que l'on a $P_a(x) = o\big(\pi(x)\big)$ quand x tend vers l'infini (Erdös, 1950). Il y a donc beaucoup moins d'entiers pseudo-premiers en base a que de nombres premiers. Par exemple, on a

$$P_2\big(10^{10}\big) = 14884 \quad \text{et} \quad \pi\big(10^{10}\big) = 455052511.$$

Un entier $n \leq 10^{10}$ étant choisi au hasard pour lequel on a $2^{n-1} \equiv 1 \bmod. n$, il y a donc moins d'une chance sur trente mille pour qu'il soit pseudo-premier et pas premier. Cela étant, pour tout $a \geq 2$, on connaît plusieurs procédés pour construire des suites infinies d'entiers pseudo-premiers en base a.

Proposition 2.1 (Cipolla, 1904). *Soit $a \geq 2$ un entier. Pour tout nombre premier $p \geq 3$ qui ne divise pas $a^2 - 1$, l'entier*

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

est pseudo-premier en base a.

Démonstration : Soit p un tel nombre premier. Posons $n = \frac{a^{2p}-1}{a^2-1}$. On vérifie directement que l'on a $a < n$. Compte tenu de l'égalité

$$n = \Big(\frac{a^p - 1}{a - 1}\Big)\Big(\frac{a^p + 1}{a + 1}\Big),$$

n est composé. Par ailleurs, on a

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

D'après le petit théorème de Fermat, on a $a^{2p} \equiv a^2 \bmod. p$. Puisque p ne divise pas $a^2 - 1$, il en résulte que p divise $n - 1$. Vu l'égalité

$$n = (a^2)^{p-1} + \cdots + a^2 + 1,$$

$n - 1$ est la somme d'un nombre pair de termes de même parité (p est impair). Par suite, $n - 1$ est pair et $2p$ divise $n - 1$. Puisque l'on a $a^{2p} \equiv 1 \bmod. n$, on en déduit que $a^{n-1} \equiv 1 \bmod. n$, d'où le résultat.

Remarque 2.1. On est resté longtemps avec l'idée que la congruence

$$2^{n-1} \equiv 1 \bmod. n \tag{4}$$

devait caractériser les entiers premiers impairs n. Ce n'est qu'en 1819 qu'on a trouvé un contre-exemple (Sarrus) avec $n = 341$. En effet, on a $n = 11 \times 31$. Par ailleurs on a $2^5 \equiv -1$ mod. 11 et $2^5 \equiv 1$ mod. 31. On obtient $2^{10} \equiv 1$ mod. n, puis $2^{n-1} \equiv 1$ mod. n.

Compte tenu de la proposition précédente, pour tout p premier ≥ 5, l'entier

$$\frac{4^p - 1}{3}$$

est pseudo-premier. Avec $p = 5$, on obtient 341, qui est le plus petit entier pseudo-premier. Signalons cependant que la condition (4) caractérise le fait pour certains entiers n d'être premiers. Par exemple, si p est premier, on a l'équivalence (exercice 5 du chapitre II)

$$2p + 1 \text{ est premier} \Longleftrightarrow 4^p \equiv 1 \text{ mod. } 2p + 1.$$

Cela fournit un critère de primalité pour les entiers de la forme $2p+1$ où p est premier. On ne sait pas démontrer l'existence d'une infinité de p premiers tels que $2p + 1$ le soit aussi.

Cipolla a aussi trouvé un procédé pour expliciter des nombres pseudo-premiers en utilisant les nombres de Fermat $F_n = 2^{2^n} + 1$.

Proposition 2.2. *Soit $n \geq 2$ un entier. L'entier*

$$\prod_{k=n}^{2^n-1} F_k$$

est pseudo-premier. En particulier, il existe des entiers pseudo-premiers qui ont un nombre arbitrairement grand de facteurs premiers.

Démonstration : Posons $r = 2^n - 1$ et $N = F_n F_{n+1} \cdots F_r$. Vérifions que l'ordre de 2 modulo N est 2^{r+1}. Pour tout $m \in \mathbb{N}$, l'ordre de 2 modulo F_m est 2^{m+1}. Deux nombres de Fermat distincts étant premiers entre eux[(1)], les groupes

$$\Big(\mathbb{Z}/N\mathbb{Z}\Big)^* \quad \text{et} \quad \prod_{k=n}^{r} \Big(\mathbb{Z}/F_k\mathbb{Z}\Big)^*$$

[(1)] Supposons $n > m$. On a

$$F_n = \big(2^{2^m}\big)^{2^{n-m}} + 1 = \big(F_m - 1\big)^{2^{n-m}} + 1 \equiv 2 \text{ mod. } F_m.$$

Par suite, tout diviseur commun de F_m et F_n divise 2, d'où l'assertion vu que F_m et F_n sont impairs. Le fait que deux nombres de Fermat distincts soient premiers entre eux entraîne par exemple qu'il existe une infinité de nombres premiers.

sont isomorphes (théorème chinois). L'ordre de 2 modulo N est ainsi le plus petit commun multiple des ordres de 2 modulo les F_k, d'où l'assertion. En particulier, on a

$$2^{2^{r+1}} \equiv 1 \text{ mod. } N. \tag{5}$$

Par ailleurs, il existe un entier impair t tel que l'on ait

$$N - 1 = 2^{2^n} t \quad \text{i.e.} \quad N - 1 = 2^{r+1} t.$$

La condition (5) entraîne alors que N est pseudo-premier. Les F_k étant premiers entre eux deux à deux, N possède au moins $2^n - n$ facteurs premiers distincts, d'où le résultat.

On peut préciser l'énoncé précédent. En 1949, Erdös a prouvé que pour tout $k \geq 2$, il existe une infinité d'entiers pseudo-premiers ayant exactement k facteurs premiers distincts.

2. Test d'Euler - Théorème de Solovay et Strassen

Rappelons que pour tout entier a et tout entier naturel impair n, on définit le symbole de Jacobi $\left(\frac{a}{n}\right)$, qui est une généralisation du symbole de Legendre. On a $\left(\frac{a}{1}\right) = 1$. Supposons $n \geq 3$. Soit $n = p_1 \cdots p_r$ la décomposition de n en produit de nombres premiers, les facteurs n'étant pas nécessairement distincts. Par définition, on pose

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

On a les égalités

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

Par ailleurs, la loi de réciprocité quadratique s'étend aux symboles de Jacobi. Autrement dit, si m et n sont des entiers naturels impairs, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ si m ou n est congru à 1 modulo 4 et sinon on a $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Si $n \geq 3$ est nombre premier, pour tout entier a, on a $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$ mod. n où $\left(\frac{a}{n}\right)$ est le symbole de Legendre (critère d'Euler). Cela étant, si n n'est pas premier, il n'y a pas de rapport en général entre le symbole de Jacobi $\left(\frac{a}{n}\right)$ et l'entier $a^{\frac{n-1}{2}}$. Par exemple, on a $\left(\frac{14}{51}\right) = 1$ et $14^{25} \equiv 20$ mod. 51. Cette remarque est à la base du test de primalité suivant :

Lemme 2.4 (Test d'Euler). *Soit $n \geq 3$ un entier impair. S'il existe un entier a tel que*

$$1 < a < n \quad \text{et} \quad \left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \text{ mod. } n,$$

alors n est composé.

Définition 2.3. *Soit $n \geq 3$ un entier impair. On appelle témoin d'Euler pour n, tout entier a premier avec n, tel que $1 < a < n$ et $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}$ mod. n.*

Définition 2.4. *Soient $n \geq 3$ un entier impair composé et a un entier premier avec n tel que $1 < a < n$. On dit que n est pseudo-premier d'Euler en base a si l'on a*

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

Un entier qui est pseudo-premier d'Euler en base 2 est appelé pseudo-premier d'Euler.

Remarques 2.2.

1) Si n est pseudo-premier d'Euler en base a, alors n est pseudo-premier en base a.

2) Le test d'Euler est plus fin que le test de Fermat. En effet, il existe des entiers n pseudo-premiers en base a, qui ne sont pas pseudo-premiers d'Euler en base a. Autrement dit, il existe des entiers n vérifiant la condition suivante : il existe un entier a tel que

$$a^{n-1} \equiv 1 \text{ mod. } n \quad \text{et} \quad \left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \text{ mod. } n.$$

Tel est le cas de l'entier $n = 341$ avec $a = 2$. En effet, on a déjà constaté que 10 est l'ordre de 2 modulo n, d'où $2^{\frac{n-1}{2}} \equiv 1$ mod. n et $2^{n-1} \equiv 1$ mod. n. Par ailleurs, on a $341 \equiv 5$ mod. 8, d'où $\left(\frac{2}{n}\right) = -1$. Ainsi, 2 est un témoin d'Euler et pas un témoin de Fermat pour n.

Comme on l'a déjà vu, il existe des entiers composés qui ne possèdent pas de témoins de Fermat, à savoir les nombres de Carmichael. On va voir maintenant qu'il n'existe pas d'entiers composés n'ayant pas de témoins d'Euler, et plus précisément qu'un entier composé n possède de nombreux témoins d'Euler, au moins $\frac{\varphi(n)}{2}$. C'est la différence essentielle entre les tests de Fermat et d'Euler. En effet, Solovay et Srassen ont établi en 1977 le résultat suivant.

Théorème 2.1 (Solovay et Strassen). *Soit $n \geq 3$ un entier impair tel que, pour tout entier a premier avec n, on ait*

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \text{ mod. } n. \tag{6}$$

Alors, n est premier.

Démonstration : On utilise ici la caractérisation des nombres de Carmichael (exercice 7 du chapitre II). Supposons que n ne soit pas premier. D'après la condition (6), pour tout entier a premier avec n, on a

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

de sorte que n est un nombre de Carmichael. Soit $n = p_1 \cdots p_r$ la décomposition de n en produit de facteurs premiers. On a $r \geq 2$ et les p_i sont distincts deux à deux (n est sans facteurs carrés). Le sous-groupe des carrés de $\mathbb{F}_{p_i}^*$ étant d'ordre $\frac{p_i-1}{2} < p_i - 1$, il existe des entiers a_i tels que l'on ait

$$\left(\frac{a_1}{p_1}\right) = -1 \quad \text{et} \quad \left(\frac{a_i}{p_i}\right) = 1 \quad \text{pour } i = 2, \cdots, r. \tag{7}$$

D'après le théorème chinois, il existe un entier a tel que l'on ait

$$a \equiv a_i \text{ mod. } p_i \quad \text{pour tout } i = 1, \cdots, r.$$

Les entiers a et n sont premiers entre eux. Vérifions alors que l'on a

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \text{ mod. } n, \tag{8}$$

ce qui entraînera le résultat. On a $\left(\frac{a}{p_i}\right) = \left(\frac{a_i}{p_i}\right)$, d'où les égalités

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a_i}{p_i}\right) = -1. \tag{9}$$

Par ailleurs, on a

$$a^{\frac{p_2-1}{2}} \equiv {a_2}^{\frac{p_2-1}{2}} \text{ mod. } p_2.$$

D'après le critère d'Euler et la condition (7), on a ${a_2}^{\frac{p_2-1}{2}} \equiv 1 \text{ mod. } p_2$. On obtient ainsi

$$a^{\frac{p_2-1}{2}} \equiv 1 \text{ mod. } p_2.$$

Puisque n est un nombre de Carmichael, $p_2 - 1$ divise $n - 1$. On en déduit que l'on a

$$a^{\frac{n-1}{2}} \equiv 1 \text{ mod. } p_2.$$

En particulier, on a

$$a^{\frac{n-1}{2}} \not\equiv -1 \text{ mod. } n.$$

Compte tenu de (9), cela établit la condition (8).

Corollaire 2.1. *Soit $n \geq 3$ un entier impair composé. L'ensemble des entiers a tels que*

$$1 < a < n, \quad \text{pgcd}(a, n) = 1 \quad \textit{et} \quad \left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \text{ mod. } n,$$

possède au moins $\frac{\varphi(n)}{2}$ éléments. Autrement dit, il y a au plus $\frac{\varphi(n)}{2}$ entiers a tels que n soit pseudo-premier d'Euler en base a.

Démonstration : L'ensemble des éléments $\overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ tels que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \text{ mod. } n$ est un sous-groupe H de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Puisque n est composé, il existe un entier a premier

avec n tel que $\overline{a}$ ne soit pas dans H (th. 2.1). L'ordre de H est donc au plus $\frac{\varphi(n)}{2}$, d'où l'assertion.

Le critère de Solovay et Strassen est un test probabiliste de primalité. Soit n un entier impair. S'il est composé, en le soumettant au test d'Euler pour une base a, on a « au moins une chance sur deux » de prouver que n est effectivement composé (cor. 2.1). Si l'on effectue k fois ce test, et que l'on constate que n passe à chaque fois le test avec succès, la probabilité pour que n soit composé est donc inférieure à $\frac{1}{2^k}$. Avec par exemple $k = 30$, n sera alors déclaré « probablement » premier, mais cela ne constitue pas une preuve de sa primalité.

Exemple 2.2. Les nombres de Fermat $F_n = 2^{2^n} + 1$ qui sont composés sont pseudo-premiers d'Euler. En effet, posons $k = 2^n - 1$. On a

$$\frac{F_n - 1}{2} = 2^k \quad \text{et} \quad k \geq n.$$

Il en résulte que l'on a

$$2^{\frac{F_n-1}{2}} = 2^{2^k} = (F_n - 1)^{2^{k-n}} \equiv (-1)^{2^{k-n}} \text{ mod. } F_n.$$

Puisque $F_0 = 3$ et $F_1 = 5$ sont premiers, on peut supposer $n \geq 2$, auquel cas on a $k > n$. On obtient alors la congruence

$$2^{\frac{F_n-1}{2}} \equiv 1 \text{ mod. } F_n.$$

Par ailleurs, F_n étant congru à 1 modulo 8, on a $\left(\frac{2}{F_n}\right) = 1$, d'où l'assertion.

3. Test de Miller

Il repose sur l'énoncé suivant.

Proposition 2.3. *Soit p un nombre premier. Posons $p - 1 = 2^s t$ avec t impair. Soit a un entier non divisible par p. Alors, on est dans l'un des cas suivants :*

1) on a $a^t \equiv 1$ mod. p.

2) Il existe un entier i tel que $0 \leq i \leq s - 1$ et $a^{2^i t} \equiv -1$ mod. p.

Démonstration : On a l'égalité

$$a^{2^s t} - 1 = (a^t - 1) \prod_{i=0}^{s-1} (a^{2^i t} + 1).$$

En effet, cette formule est vraie si $s = 0$ (un produit vide vaut 1). Si on la suppose vérifiée pour $s \in \mathbb{N}$, alors elle l'est aussi pour $s + 1$, vu que $a^{2^{s+1} t} - 1 = \left(a^{2^s t}\right)^2 - 1$. D'après le petit théorème de Fermat, p divise $a^{p-1} - 1$, d'où le résultat.

On obtient le test de primalité de Miller :

Corollaire 2.2 (Test de Miller). *Soit $n \geq 3$ un entier impair. Posons $n-1 = 2^s t$ avec t impair. Supposons qu'il existe un entier a, avec $1 < a < n$, tel que l'on ait*

$$a^t \not\equiv 1 \text{ mod. } n \quad \text{et} \quad a^{2^i t} \not\equiv -1 \text{ mod. } n \quad \text{pour tout } i \in \Big\{0, \cdots, s-1\Big\}. \tag{10}$$

Alors, n est composé.

Définition 2.5. *Soit $n \geq 3$ un entier impair. On appelle témoin de Miller pour n, tout entier a premier avec n, tel que $1 < a < n$, vérifiant la condition* (10).

Exemple 2.3. Rappelons que 561 est un nombre de Carmichael (c'est le plus petit). On a $560 = 2^4 \times 35$. On vérifie que l'on a $2^{35} \equiv 263$ mod. 561, et que

$$2^{2.35} \equiv 166 \text{ mod. } 561, \quad 2^{2^2.35} \equiv 67 \text{ mod. } 561, \quad 2^{2^3.35} \equiv 1 \text{ mod. } 561.$$

Par suite, 2 est un témoin de Miller pour 561. Ce n'est pas un témoin d'Euler pour 561.

Définition 2.6. *Soit $n \geq 3$ un entier impair composé. Posons $n-1 = 2^s t$ avec t impair. Soit a un entier tel que $1 < a < n$. On dit que n est pseudo-premier fort en base a si l'une des conditions suivantes est satisfaite :*

1) on a $a^t \equiv 1$ mod. n.

2) Il existe un entier i tel que $0 \leq i \leq s-1$ et $a^{2^i t} \equiv -1$ mod. n.

Un entier pseudo-premier fort en base 2 est appelé pseudo-premier fort.

Exemple 2.4. Les nombres de Fermat $F_n = 2^{2^n} + 1$ qui sont composés sont pseudo-premiers forts, vu que l'on a $2^{2^n} \equiv -1$ mod. F_n, et la seconde condition de la définition 2.6 est donc satisfaite avec l'entier $i = n$ (on a $s = 2^n$ et $t = 1$).
Le plus petit entier pseudo-premier fort est 2047. Le plus petit entier pseudo-premier fort en bases 2 et 3 est 1373653.

En 1980, Pomerance, Selfridge et Wagstaff ont démontré que pour tout $a > 1$, il existe une infinité d'entiers pseudo-premiers forts en base a. On peut donner une preuve directe de ce résultat si $a = 2$.

Lemme 2.5. *Si n est un entier pseudo-premier, alors $2^n - 1$ est pseudo-premier fort. En particulier, il existe une infinité d'entiers pseudo-premiers forts.*

Démonstration : Soit $n \geq 2$ un entier pseudo-premier. Posons $M_n = 2^n - 1$. Puisque n est composé, il en est de même de M_n. On a $M_n - 1 = 2t$ avec t impair. Par ailleurs, on a $2^{n-1} \equiv 1$ mod. n, autrement dit, n divise $\frac{M_n - 1}{2}$. Il en résulte que l'on a

$$2^{\frac{M_n-1}{2}} - 1 \equiv 0 \text{ mod. } M_n.$$

On obtient la congruence

$$2^t \equiv 1 \text{ mod. } M_n,$$

ce qui prouve que M_n est pseudo-premier fort. Cela entraîne le résultat vu qu'il existe une infinité d'entiers pseudo-premiers (prop. 2.1).

Explicitons une autre suite infinie d'entiers pseudo-premiers forts.

Lemme 2.6. *Pour tout nombre premier $p \geq 7$, l'entier $\frac{4^p+1}{5}$ est pseudo-premier fort.*

Démonstration : Posons $n = \frac{4^p+1}{5}$ où p est premier ≥ 7. L'entier $4^p + 1$ est divisible par 5, donc n est un entier. L'égalité

$$4^p + 1 = \big(2^p - 2^{\frac{p+1}{2}} + 1\big)\big(2^p + 2^{\frac{p+1}{2}} + 1\big),$$

entraîne que n est composé. Par ailleurs, on a $n - 1 = 4t$ où t est impair. Vu que $p \geq 7$, l'entier t est multiple de p (petit théorème de Fermat). Puisque l'on a $2^{2p} \equiv -1$ mod. n, on obtient alors

$$2^{2t} \equiv -1 \text{ mod. } n,$$

et la seconde condition de la définition 2.6 est satisfaite (avec $a = 2$ et $i = 1$).

Voyons maintenant le lien qui existe entre la notion d'entier pseudo-premier fort et celle d'entier pseudo-premier d'Euler dans une base fixée. Tout d'abord, pour les entiers congrus à 3 modulo 4, ces notions sont les mêmes.

Lemme 2.7. *Soit n un entier congru à 3 modulo 4. Alors, n est pseudo-premier fort en base a si et seulement si n est pseudo-premier d'Euler en base a.*

Démonstration : On a $n - 1 \equiv 2$ mod. 4. Il existe donc un entier impair t tel que l'on ait $n - 1 = 2t$. Si n est composé, il en résulte que l'on a l'équivalence

$$n \text{ est pseudo-premier fort en base } a \iff a^{\frac{n-1}{2}} \equiv \pm 1 \text{ mod. } n. \tag{11}$$

Supposons que n soit pseudo-premier d'Euler en base a. Dans ce cas, on a

$$\pm 1 = \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \text{ mod. } n,$$

et d'après (11), n est pseudo-premier fort en base a. Inversement, supposons n pseudo-premier fort en base a. Compte tenu de la congruence $n \equiv 3$ mod. 4, on a les égalités

$$\left(\frac{a}{n}\right) = \left(\frac{a\big(a^2\big)^{\frac{n-3}{4}}}{n}\right) = \left(\frac{a^{\frac{n-1}{2}}}{n}\right).$$

D'après l'hypothèse faite et l'équivalence (11), on a $a^{\frac{n-1}{2}} \equiv \pm 1$ mod. n. Si l'on a la congruence $a^{\frac{n-1}{2}} \equiv 1$ mod. n, on obtient $\left(\frac{a}{n}\right) = 1$, d'où le résultat dans ce cas. Si on a $a^{\frac{n-1}{2}} \equiv -1$ mod. n, vu que $n \equiv 3$ mod. 4, on obtient alors

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

On a ainsi $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ mod. n, autrement dit, n est pseudo-premier d'Euler en base a.

En toute généralité, on a l'énoncé suivant :

Proposition 2.4. *Soit n un entier pseudo-premier fort en base a. Alors, n est pseudo-premier d'Euler en base a.*

Démonstration : Posons $n - 1 = 2^s t$ avec t impair. L'entier n étant impair ≥ 3, on a $s \geq 1$. L'une des deux conditions de la définition 2.6 est satisfaite.

Supposons $a^t \equiv 1$ mod. n. D'après l'égalité $\frac{n-1}{2} = 2^{s-1}t$, on obtient la congruence

$$a^{\frac{n-1}{2}} \equiv 1 \text{ mod. } n.$$

Par ailleurs, t étant impair, on a les égalités

$$\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^t = \left(\frac{a^t}{n}\right) = 1.$$

Cela prouve que n est pseudo-premier d'Euler en base a.

Supposons qu'il existe un entier i tel que $0 \leq i \leq s-1$ et $a^{2^i t} \equiv -1$ mod. n. Si l'on a $i < s - 1$, on a

$$a^{\frac{n-1}{2}} = a^{2^{s-1}t} = \left(a^{2^i t}\right)^{2^{s-1-i}} \equiv 1 \text{ mod. } n.$$

Si l'on a $i = s - 1$, on obtient dans ce cas

$$a^{\frac{n-1}{2}} = a^{2^{s-1}t} \equiv -1 \text{ mod. } n.$$

Par suite, il s'agit de démontrer que l'on a

$$\left(\frac{a}{n}\right) = 1 \quad \text{si} \quad i < s-1 \quad \text{et} \quad \left(\frac{a}{n}\right) = -1 \quad \text{si} \quad i = s-1. \tag{12}$$

Considérons pour cela un diviseur premier p de n. Posons $p - 1 = 2^u v$ avec v impair. Vérifions que la condition suivante est satisfaite : on a

$$u \geq i+1 \quad \text{avec} \quad \left(\frac{a}{p}\right) = 1 \quad \text{si} \quad u > i+1 \quad \text{et} \quad \left(\frac{a}{p}\right) = -1 \quad \text{si} \quad u = i+1. \tag{13}$$

On a $a^{2^i t} \equiv -1$ mod. p. Puisque v est impair, on a donc

$$a^{2^i tv} \equiv -1 \text{ mod. } p. \tag{14}$$

On a $a^{2^{u-1}v} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ mod. p (critère d'Euler). L'entier t étant impair, on obtient

$$a^{2^{u-1}vt} \equiv \left(\frac{a}{p}\right) \text{ mod. } p. \tag{15}$$

Les congruences (14) et (15) impliquent alors la condition (13).
Si l'on a $u > i+1$, alors $p \equiv 1$ mod. 2^{i+2}. Si $u = i+1$, on a $p \equiv 1+2^{i+1}$ mod. 2^{i+2}. Notons alors k le nombre de diviseurs premiers de n, comptés avec leurs multiplicités, pour lesquels on a $u = i+1$. On obtient

$$\left(\frac{a}{n}\right) = \prod_p \left(\frac{a}{p}\right) = (-1)^k \quad \text{et} \quad n \equiv \left(1+2^{i+1}\right)^k \text{ mod. } 2^{i+2},$$

où dans le produit, p parcourt l'ensemble des diviseurs premiers de n comptés avec multiplicités. Puisque l'on a $\left(1+2^{i+1}\right)^k \equiv 1 + k2^{i+1}$ mod. 2^{i+2}, il en résulte que

$$n \not\equiv 1 \text{ mod. } 2^{i+2} \quad \text{si} \quad k \equiv 1 \text{ mod. } 2 \quad \text{et} \quad n \equiv 1 \text{ mod. } 2^{i+2} \quad \text{si} \quad k \equiv 0 \text{ mod. } 2.$$

On a $n-1 = 2^s t$ avec t impair et $s \geq i+1$. On en déduit que l'on a

$$s = i+1 \quad \text{si} \quad k \equiv 1 \text{ mod. } 2 \quad \text{et} \quad s > i+1 \quad \text{si} \quad k \equiv 0 \text{ mod. } 2.$$

L'égalité $\left(\frac{a}{n}\right) = (-1)^k$ entraîne alors la condition (12), d'où le résultat.

Remarque 2.3. Il existe des entiers congrus à 1 modulo 4 qui sont pseudo-premiers d'Euler et qui ne sont pas pseudo-premiers forts. Tel est le cas de l'entier $n = 1105$. En effet, on a $n \equiv 1$ mod. 8, d'où $\left(\frac{2}{n}\right) = 1$. Par ailleurs, on a $n-1 = 2^4 \times 69$ et l'on vérifie la congruence

$$2^{\frac{n-1}{2}} \equiv 1 \text{ mod. } n.$$

Ainsi, n est pseudo-premier d'Euler. Par ailleurs, on a

$$2^{69} \equiv 967 \text{ mod. } n, \quad 2^{2.69} \equiv 259 \text{ mod. } n, \quad 2^{2^2.69} \equiv 781 \text{ mod. } n, \quad 2^{2^3.69} \equiv 1 \text{ mod. } n.$$

L'entier n n'est donc pas pseudo-premier fort.

4. Théorème de Rabin

Il s'agit de l'énoncé suivant, établi en 1980 par Rabin.

Théorème 2.2 (Rabin). *Soit $n \geq 11$ un entier impair composé. Soit $S(n)$ le sous-ensemble de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ formé des éléments $a + n\mathbb{Z}$ tels que n soit pseudo-premier fort en base a. Alors, on a*

$$|S(n)| \leq \frac{\varphi(n)}{4}.$$

Autrement dit, si $n \geq 11$ est un entier impair composé, il y a au plus $\varphi(n)/4$ entiers a tels que n soit pseudo-premier fort en base a. Compte tenu de ce résultat, et de la proposition 2.4, le test de Miller est un test probabiliste de primalité qui améliore le test d'Euler. Étant donné un entier n, s'il est composé, en le soumettant au test de Miller, on a « au moins trois chances sur quatre » de démontrer que tel est bien le cas. En effectuant k fois ce test, si l'on constate que n passe à chaque fois le test avec succès, la probabilité pour que n soit composé est donc inférieure à $\frac{1}{4^k}$. Avec par exemple $k = 20$, n sera déclaré « probablement » premier. Le test de Miller est très performant. Il permet de détecter rapidement des nombres premiers ayant plusieurs centaines de chiffres décimaux.

Démonstration du théorème : Posons

$$n - 1 = 2^s t \quad \text{avec } t \text{ impair.}$$

Notons $\nu(n)$ le plus grand entier satisfaisant la condition suivante : pour chaque diviseur premier p de n, $2^{\nu(n)}$ divise $p - 1$. Puisque n est impair, on a $\nu(n) \geq 1$.

Lemme 2.8. *Supposons n pseudo-premier fort en base a. Alors, on a*

$$a^{2^{\nu(n)-1}t} \equiv \pm 1 \text{ mod. } n.$$

Démonstration : Si l'on a $a^t \equiv 1$ mod. n, l'assertion est vérifiée. Supposons donc qu'il existe un entier i tel que

$$a^{2^i t} \equiv -1 \text{ mod. } n \quad \text{et} \quad 0 \leq i \leq s - 1.$$

Soit p un diviseur premier de n. Notons r l'ordre multiplicatif de a modulo p. D'après la congruence précédente, on a

$$a^{2^{i+1}t} \equiv 1 \text{ mod. } n.$$

Par suite, r divise $2^{i+1}t$ et ne divise pas $2^i t$. Il en résulte que $i+1$ est l'exposant de 2 dans la décomposition de r en facteurs premiers. Par ailleurs, on a $a^{p-1} \equiv 1$ mod. p (d'après l'hypothèse faite, a est premier avec n, donc p ne divise pas a). Ainsi r divise $p - 1$. On en déduit que l'on a

$$p - 1 \equiv 0 \text{ mod. } 2^{i+1}.$$

Puisque cette congruence vaut pour tout diviseur premier de n, on obtient

$$i + 1 \leq \nu(n).$$

Par suite, $a^{2^{\nu(n)-1}t}$ est congru à 1 ou -1 modulo n, suivant que l'on a $i+1 < \nu(n)$ ou $i+1 = \nu(n)$, d'où le résultat.

Soit $T(n)$ le sous-ensemble de $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$ formé des éléments $a+n\mathbb{Z}$ tels que

$$a^{2^{\nu(n)-1}t} \equiv \pm 1 \text{ mod. } n.$$

Lemme 2.9. *Soit $\omega(n)$ le nombre de diviseurs premiers distincts de n. On a*

$$|T(n)| = 2^{(\nu(n)-1)\omega(n)+1} \prod_{p|n} \operatorname{pgcd}(t, p-1),$$

où p parcourt l'ensemble des diviseurs premiers de n.

Démonstration : Posons $m = 2^{\nu(n)-1}t$ et $k = \omega(n)$. Notons

$$n = p_1^{j_1} \cdots p_k^{j_k},$$

la décomposition en facteurs premiers distincts de n. Soit $T'(n)$ le sous-ensemble de $T(n)$ formé des éléments $a+n\mathbb{Z}$ tels que

$$a^m \equiv 1 \text{ mod. } n.$$

Démontrons que l'on a

$$|T'(n)| = 2^{(\nu(n)-1)\omega(n)} \prod_{i=1}^{k} \operatorname{pgcd}(t, p_i - 1). \tag{16}$$

Un élément $a+n\mathbb{Z} \in \big(\mathbb{Z}/n\mathbb{Z}\big)^*$ appartient à $T'(n)$ si et seulement si on a $a^m \equiv 1$ mod. $p_i^{j_i}$ pour tout $i = 1, \cdots, k$. Par ailleurs, p_i étant impair, le groupe $\big(\mathbb{Z}/p_i^{j_i}\mathbb{Z}\big)^*$ est cyclique d'ordre $p_i^{j_i-1}(p_i-1)$. Le nombre de solutions de l'équation $x^m = 1$ dans ce groupe est donc

$$\operatorname{pgcd}\big(m, p_i^{j_i-1}(p_i-1)\big).$$

Parce que p_i ne divise pas m, et d'après la définition des entiers m et $\nu(n)$, on a

$$\operatorname{pgcd}\big(m, p_i^{j_i-1}(p_i-1)\big) = \operatorname{pgcd}(m, p_i-1) = 2^{\nu(n)-1} \operatorname{pgcd}(t, p_i-1).$$

Le théorème chinois entraîne alors l'égalité (16). Soit $T''(n)$ le sous-ensemble de $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$ formé des éléments $a+n\mathbb{Z}$ tels que

$$a^m \equiv -1 \text{ mod. } n.$$

Puisque $T(n)$ est la réunion disjointe de $T'(n)$ et $T''(n)$, tout revient à prouver que l'on a

$$|T'(n)| = |T''(n)|. \tag{17}$$

Un élément $a + n\mathbb{Z} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ appartient à $T''(n)$ si et seulement si on a

$$a^m \equiv -1 \text{ mod. } p_i^{j_i}$$

pour tout $i = 1, \cdots, k$. Le groupe $\left(\mathbb{Z}/p_i^{j_i}\mathbb{Z}\right)^*$ étant cyclique, l'équation $x^2 = 1$ a exactement deux solutions à savoir ± 1. Par suite, cette condition signifie que l'on a

$$a^{2m} \equiv 1 \text{ mod. } p_i^{j_i} \quad \text{et} \quad a^m \not\equiv 1 \text{ mod. } p_i^{j_i}.$$

En utilisant le même argument que celui évoqué ci-dessus, on vérifie que le nombre d'éléments x de $\left(\mathbb{Z}/p_i^{j_i}\mathbb{Z}\right)^*$ tels que $x^{2m} = 1$ et $x^m \neq 1$ est

$$2^{\nu(n)} \operatorname{pgcd}(t, p_i - 1) - 2^{\nu(n)-1} \operatorname{pgcd}(t, p_i - 1) = 2^{\nu(n)-1} \operatorname{pgcd}(t, p_i - 1).$$

Cela implique l'égalité (17) (théorème chinois), d'où le lemme.

Le théorème de Rabin se déduit comme suit. D'après le lemme 2.8, il suffit de prouver que l'on a

$$|T(n)| \leq \frac{\varphi(n)}{4}. \tag{18}$$

D'après le lemme 5.9, on a

$$\frac{\varphi(n)}{|T(n)|} = \frac{1}{2} \prod_{p^\alpha || n} p^{\alpha-1} \frac{p-1}{2^{\nu(n)-1} \operatorname{pgcd}(t, p-1)}, \tag{19}$$

où la notation $p^\alpha || n$ signifie que α est l'exposant de p dans la décomposition de n en facteurs premiers. Pour chaque diviseur premier p de n,

$$\frac{p-1}{2^{\nu(n)-1} \operatorname{pgcd}(t, p-1)}$$

est un entier pair (par définition de $\nu(n)$) de sorte que $\frac{\varphi(n)}{|T(n)|}$ est un entier. On déduit alors de (19) que l'on a

$$\frac{\varphi(n)}{|T(n)|} \geq 4 \quad \text{si} \quad \omega(n) \geq 3.$$

Si l'on a $\omega(n) = 2$ et si n possède au moins un facteur carré, on a

$$\prod_{p^\alpha || n} p^{\alpha-1} \geq 3, \quad \text{d'où} \quad \frac{\varphi(n)}{|T(n)|} \geq 6.$$

Supposons $\omega(n) = 2$ et n sans facteurs carrés. On a alors $n = pq$ où p et q sont premiers avec $p < q$. Si $2^{\nu(n)+1}$ divise $q-1$, on obtient

$$\frac{q-1}{2^{\nu(n)-1}\,\mathrm{pgcd}(t,q-1)} \geq 4, \quad \text{d'où} \quad \frac{\varphi(n)}{|T(n)|} \geq 4.$$

On peut donc supposer que l'exposant de 2 dans la décomposition de $q-1$ en facteurs premiers est exactement $\nu(n)$. On a $n-1 = pq-1 = (p-1)+p(q-1)$, d'où la congruence $n-1 \equiv p-1$ mod. $q-1$. Par suite, $q-1$ ne divise pas $n-1$ (sinon on aurait $q \leq p$). L'entier $2^{\nu(n)}$ divise $p-1$ et $q-1$, donc il divise $n-1$. On en déduit l'existence d'un nombre premier impair ℓ et d'un entier h tels que l'on ait

$$q-1 \equiv 0 \text{ mod. } \ell^h \quad \text{et} \quad n-1 \not\equiv 0 \text{ mod. } \ell^h.$$

L'entier ℓ^h ne divisant pas t, on a l'inégalité

$$\frac{q-1}{2^{\nu(n)-1}\,\mathrm{pgcd}(t,q-1)} \geq 6.$$

On obtient donc dans ce cas

$$\frac{\varphi(n)}{|T(n)|} \geq 6.$$

Il reste à traiter le cas où n est une puissance d'un nombre premier p. Posons $n = p^a$ avec $a \geq 2$. On a

$$p-1 = 2^{\nu(n)}u \quad \text{avec} \quad u \equiv 1 \text{ mod. } 2 \quad \text{et} \quad |T(n)| = 2^{\nu(n)}\,\mathrm{pgcd}(t,p-1).$$

On a $\mathrm{pgcd}(t,p-1) = \mathrm{pgcd}(t,u)$. Par ailleurs, $p-1$ divise $n-1 = 2^s t$, donc u divise t. On en déduit que l'on a

$$|T(n)| = 2^{\nu(n)}u = p-1 \quad \text{d'où} \quad \frac{\varphi(n)}{|T(n)|} = p^{a-1},$$

ce qui conduit à l'inégalité

$$\frac{\varphi(n)}{|T(n)|} \geq 5 \quad \text{si} \quad n \neq 9.$$

Cela prouve la condition (18) et termine la démonstration du théorème.

Remarque 2.4. Étant donné un entier impair composé $n \geq 3$, notons $W(n)$ le plus petit témoin de Miller pour n. On a très souvent $W(n) = 2$, car si n est pseudo-premier fort, il est en particulier pseudo-premier, et comme on l'a vu de tels entiers sont assez rares. Cela étant, d'après le lemme 2.6, il existe une infinité d'entiers n tels que l'on ait $W(n) \geq 3$. Par ailleurs, on a $W(n) \leq \sqrt{n}$ vu qu'il existe un diviseur premier p de n plus petit que $\sqrt{n}$ et la condition (10) est donc satisfaite avec l'entier $a = p$. Une conjecture

en théorie des nombres, appelée l'hypothèse de Riemann généralisée, entraîne en fait que l'on a

$$W(n) \leq 2(\log n)^2.$$

Signalons que dans le cas où n est divisible par le carré d'un nombre premier, on peut démontrer, sans utiliser de conjecture, que l'on a $W(n) < (\log n)^2$.

Remarque 2.5. Soit $n \geq 3$ un entier composé impair. Supposons que l'on connaisse un entier a tel que n soit pseudo-premier en base a, et ne soit pas pseudo-premier fort en base a. Alors, on peut trouver rapidement un diviseur non trivial de n. En effet, posons $n-1 = 2^s t$ avec t impair et considérons l'ensemble

$$A = \left\{ k \in \mathbb{N} \;\middle|\; 0 \leq k \leq s \quad \text{et} \quad a^{\frac{n-1}{2^k}} \not\equiv 1 \text{ mod. } n \right\}.$$

Il n'est pas vide car n n'étant pas pseudo-premier fort en base a, l'entier s appartient à A. Soit r le plus petit élément de A. Posons

$$b = a^{\frac{n-1}{2^r}} = a^{2^{s-r}t}.$$

On a donc $b \not\equiv 1$ mod. n car $r \in A$. Puisque n est pseudo-premier en base a, on a la congruence $a^{n-1} \equiv 1$ mod. n, par suite on a $r \geq 1$. Les inégalités $0 \leq s-r \leq s-1$ impliquent alors $b \not\equiv -1$ mod. n. Par ailleurs, on a

$$b^2 = a^{\frac{n-1}{2^{r-1}}}.$$

L'entier naturel $r-1$ n'étant pas dans A, on a donc $b^2 \equiv 1$ mod. n. On obtient ainsi

$$b \not\equiv \pm 1 \text{ mod. } n \quad \text{et} \quad b^2 \equiv 1 \text{ mod. } n.$$

L'entier $c = \text{pgcd}(b+1, n)$ est distinct de 1 et n, c'est donc un diviseur non trivial de n.

Remarque 2.6 (Sur le cryptosystème RSA). Supposons que l'on ait $n = pq$ où p et q sont nombres premiers impairs distincts. Posons

$$d = \text{pgcd}(p-1, q-1).$$

L'égalité $n-1 = (p-1)q + (q-1)$ implique

$$d = \text{pgcd}(n-1, p-1) = \text{pgcd}(n-1, q-1).$$

D'après le lemme 2.3, il y a donc exactement $d^2 - 1$ entiers a tels que n soit pseudo-premier en base a. Dans l'utilisation du cryptosystème RSA, il convient donc de choisir p et q de sorte que d soit petit. Comme annoncé dans le chapitre I, c'est l'une des précautions à

prendre sur le choix de p et q. Sinon, on peut trouver assez facilement un entier a tel que n soit pseudo-premier en base a. Vu l'efficacité du test de Miller, il y aura de grandes chances pour que n ne soit pas pseudo-premier fort en base a. Compte tenu de la remarque précédente, cela permet alors de trouver rapidement la factorisation de n.

Prenons par exemple $n = 273645221$. On vérifie que n est pseudo-premier en base 32 (il ne l'est pas pour les entiers < 32) et que n n'est pas pseudo-premier fort en base 32. Par ailleurs, on a

$$n - 1 = 2^2 t \quad \text{avec} \quad t = 5.19^2.151.251,$$

de sorte que, avec les notations utilisées dans la remarque 2.5, on a

$$b = 32^{2t} \quad \text{et} \quad c = \text{pgcd}(b + 1, n) = 15101.$$

On obtient ainsi l'égalité

$$n = pq \quad \text{avec} \quad p = 15101 \quad \text{et} \quad q = 18121,$$

qui sont des nombres premiers. On notera que l'on a $\text{pgcd}(p - 1, q - 1) = 3020$.

5. Critère de primalité de Lehmer

Il s'agit d'un critère de primalité concernant les entiers n pour lesquels on connaît les diviseurs premiers de $n - 1$.

Proposition 2.5 (Critère de Lehmer, 1927). *Soit $n \geq 3$ un entier impair. Les conditions suivantes sont équivalentes :*

1) n est premier.

2) Il existe un entier a tel que l'on ait

$$a^{n-1} \equiv 1 \text{ mod. } n \quad \textit{et} \quad a^{\frac{n-1}{q}} \not\equiv 1 \text{ mod. } n, \tag{20}$$

pour tout diviseur premier q de $n - 1$.

Démonstration : Si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps et le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est cyclique. Si $a + n\mathbb{Z}$ est un générateur de ce groupe, la seconde condition est satisfaite avec l'entier a. Inversement, soit a un entier pour lequel cette condition soit réalisée. Puisque a est premier avec n, l'élément $a+n\mathbb{Z}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. Dans le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, l'ordre de $a+n\mathbb{Z}$ est $n-1$[(2)]. Il en résulte que $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est d'ordre $n-1$. On a donc $\varphi(n) = n-1$, ce qui entraîne que n est premier.

Exemple 2.5. Ce critère, utilisé avec $a = 5$, permet de démontrer que $3.2^{3189} + 1$ est premier. Cet entier possède neuf cent soixante et un chiffres décimaux.

Corollaire 2.3. *Soit $n \geq 3$ un entier impair. Les conditions suivantes sont équivalentes :*

1) n est premier.

2) Il existe un entier a tel que l'on ait

$$a^{\frac{n-1}{2}} \equiv -1 \text{ mod. } n \quad et \quad a^{\frac{n-1}{q}} \not\equiv 1 \text{ mod. } n, \tag{21}$$

pour tout diviseur premier impair q de $n-1$.

Démonstration : Supposons n premier. Soit a un entier satisfaisant la condition (20). Puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps, la congruence $a^{n-1} \equiv 1$ mod. n entraîne $a^{\frac{n-1}{2}} \equiv \pm 1$ mod. n, d'où $a^{\frac{n-1}{2}} \equiv -1$ mod. n, et la condition (21) est satisfaite avec a. Inversement, il est immédiat que si (21) est réalisée avec un entier a, alors (20) l'est aussi avec a, donc n est premier.

On peut affiner ces résultats avec celui obtenu par Brillhart et Selfridge en 1967 :

Proposition 2.6. *Soit $n \geq 2$ un entier. Supposons que pour tout diviseur premier q de $n-1$, il existe un entier a, qui dépend de q, tel que l'on ait*

$$a^{n-1} \equiv 1 \text{ mod. } n \quad et \quad a^{\frac{n-1}{q}} \not\equiv 1 \text{ mod. } n.$$

Alors, n est premier.

Démonstration : Il suffit de prouver que l'on a $\varphi(n) = n - 1$. Puisque $\varphi(n) \leq n - 1$, il suffit donc d'établir que $n - 1$ divise $\varphi(n)$. Considérons pour cela un nombre premier q et un entier $r \geq 1$ tels que q^r divise $n - 1$. Vérifions que q^r divise $\varphi(n)$. Par hypothèse, il existe un entier a tel que l'on ait $a^{n-1} \equiv 1$ mod. n et $a^{\frac{n-1}{q}} \not\equiv 1$ mod. n. L'entier a est premier avec n. Soit d l'ordre de la classe de a dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$. On a

$$n - 1 \equiv 0 \text{ mod. } d \quad \text{et} \quad \frac{n-1}{q} \not\equiv 0 \text{ mod. } d.$$

---

(2) On utilise ici le résultat suivant. Soient G un groupe fini, d'élément neutre e, et x un élément de G. Soit $m \geq 1$ un entier. Alors, x est d'ordre m si et seulement si on a $x^m = e$ et pour tout diviseur premier p de m, on a $x^{\frac{m}{p}} \neq e$. Vérifions l'implication la moins immédiate. Notons d l'ordre de x. Il existe un entier $k \geq 1$ tel que l'on ait $m = dk$. Supposons $k \geq 2$. Soit p un diviseur premier de k. On a alors les égalités

$$x^{\frac{m}{p}} = \left(x^d\right)^{\frac{k}{p}} = e,$$

ce qui contredit l'hypothèse faite. Par suite, on a $k = 1$, puis $m = d$.

Posons $n-1=kd$. L'entier q ne divise pas k, donc q^r divise d. Par ailleurs, la congruence $a^{\varphi(n)} \equiv 1$ mod. n entraîne que d divise $\varphi(n)$. Ainsi q^r divise $\varphi(n)$, d'où le fait que $n-1$ divise $\varphi(n)$, et le résultat.

Exemple 2.6. On peut démontrer que $3.2^{2816}+1$ est premier en utilisant ce critère avec les couples $(q,a)=(2,7)$ et $(3,2)$, ou bien la proposition 2.5, avec $a=13$.

En utilisant ce qui précède, on obtient un critère de primalité dû à Pepin pour les nombres de Fermat.

Proposition 2.7 (Test de Pepin, 1877). *Soit $n \geq 1$ un entier. Posons $F_n = 2^{2^n}+1$. On a l'équivalence*

$$F_n \text{ est premier } \iff 3^{\frac{F_n-1}{2}} \equiv -1 \text{ mod. } F_n.$$

Démonstration : Si l'on a $3^{\frac{F_n-1}{2}} \equiv -1$ mod. F_n, la condition (21) est satisfaite par F_n avec $a=3$, donc F_n est premier. Inversement, supposons F_n premier. Puisque 2^n est pair, on a $2^{2^n} \equiv 1$ mod. 3 d'où $F_n \equiv 2$ mod. 3. Par ailleurs, on a $F_n \equiv 1$ mod. 4. On en déduit les égalités

$$\Big(\frac{3}{F_n}\Big) = \Big(\frac{F_n}{3}\Big) = -1.$$

Le critère d'Euler entraîne alors le résultat.

Exemple 2.7. Pour tout n tel que $5 \leq n \leq 32$, l'entier F_n est composé. On ignore si F_{33} est composé. Avec un MacBookPro et le logiciel de calculs Pari, le temps d'exécution de ce test pour démontrer que F_{16} est composé est d'environ une minute. Son temps d'exécution pour établir que F_{17} est composé est d'environ sept minutes. En utilisant le fait que tout diviseur premier de F_n est congru à 1 modulo 2^{n+1} (et même modulo 2^{n+2}), on peut facilement démontrer que certains F_n sont composés pour n de l'ordre de 10^5. Par exemple, on peut vérifier en trois minutes que F_{95328} est divisible par $7.2^{95330}+1$.

Considérons un entier impair $n \geq 3$. Il arrive que l'on connaisse seulement une factorisation partielle de l'entier $n-1$. Si la partie connue de cette factorisation est suffisamment grande en fonction de n, cela est parfois suffisant pour démontrer que n est premier si tel est le cas. Voyons quelques résultats dans cette direction.

Supposons que l'on ait une égalité de la forme

$$n-1 = FR, \tag{22}$$

où en pratique la décomposition de F en facteurs premiers est connue.

Théorème 2.3 (Pocklington, 1914). *Supposons qu'il existe un entier a tel que, pour tout diviseur premier q de F, on ait*

$$a^{n-1} \equiv 1 \text{ mod. } n \quad et \quad \text{pgcd}\Big(a^{\frac{n-1}{q}} - 1, n\Big) = 1. \tag{23}$$

Alors, les deux assertions suivantes sont satisfaites :

1) chaque diviseur premier de n est congru à 1 modulo F.

2) Si l'on a $F \geq \sqrt{n}$, alors n est premier.

Démonstration : 1) Soit p un diviseur premier de n. L'entier a est premier avec n. Soit d l'ordre de a^R modulo p. On a $a^{FR} \equiv 1$ mod. p, donc d divise F. Supposons $d \neq F$. Dans ce cas, il existe un entier $k \geq 2$ tel que l'on ait $F = kd$, d'où $n - 1 = kdR$. Si q est un diviseur premier de k, alors dR divise $\frac{n-1}{q}$, d'où $a^{\frac{n-1}{q}} \equiv 1$ mod. p, ce qui conduit à une contradiction. On a donc $d = F$, par suite F divise $p - 1$.
2) Chaque diviseur premier de n est strictement plus grand que F. D'après l'hypothèse faite, chaque diviseur premier de n est donc strictement plus grand que $\sqrt{n}$, ce qui entraîne que n est premier.

On retrouve un critère de primalité pour les entiers de la forme $h2^N + 1$ avec $h < 2^N$ (en pratique h est impair). Ces entiers s'appellent les nombres de Proth.

Corollaire 2.4 (Proth, 1878). *Soient $h, N \geq 1$ des entiers tels que $h < 2^N$. Posons $n = h2^N + 1$. Soit a un entier tel que $\left(\frac{a}{n}\right) = -1$. On a l'équivalence*

$$n \text{ est premier } \iff a^{\frac{n-1}{2}} \equiv -1 \text{ mod. } n.$$

Démonstration : Supposons n premier. D'après le critère d'Euler et l'hypothèse faite on a $a^{\frac{n-1}{2}} \equiv -1$ mod. n. Inversement, on a $a^{n-1} \equiv 1$ mod. n et $\text{pgcd}\big(a^{\frac{n-1}{2}} - 1, n\big) = 1$ (car n est impair). On a $n - 1 = h2^N < 2^{2N}$ i.e. $n \leq 2^{2N}$, d'où $\sqrt{n} \leq 2^N$. Le théorème 2.3, utilisé avec $F = 2^N$, entraîne alors que n est premier.

Exemple 2.8. Posons $n = 3.2^N + 1$ avec N non multiple de 4. Vérifions l'équivalence

$$n \text{ est premier } \iff 5^{\frac{n-1}{2}} \equiv -1 \text{ mod. } n.$$

Si N est congru à 3 modulo 4, alors 5 divise n. Dans ce cas, n n'est pas premier (car $n > 5$) et l'équivalence est vraie. Si N est congru à 1 (resp. 2) modulo 4, alors n est congru 2 (resp. 3) modulo 5, d'où $\left(\frac{5}{n}\right) = -1$ et l'assertion (cor. 2.4).
Le cas où N est multiple de 4 se traduit moins facilement. Supposons $N = 4k$ avec $k \equiv 3$ mod. 5. On a alors $n \equiv 2$ mod. 11, par suite

$$n \text{ est premier } \iff 11^{\frac{n-1}{2}} \equiv -1 \text{ mod. } n.$$

Avec ce critère, on constate que $3.2^{3912} + 1$ est premier. Il possède 1179 chiffres décimaux.

Exemple 2.9. Pour tout $n \geq 1$ posons

$$t_n = 2^{2^n} - 2^{2^{n-1}} + 1.$$

On a $t_1 = 3$, $t_2 = 13$, $t_3 = 241$. Supposons $n \geq 2$. Vérifions que l'on a l'équivalence

$$t_n \text{ est premier} \Longleftrightarrow 7^{\frac{t_n-1}{2}} \equiv -1 \text{ mod. } t_n. \tag{24}$$

Supposons t_n premier. On vérifie que l'on a

$$t_n \equiv 3 \text{ mod. } 7 \quad \text{si } n \equiv 1 \text{ mod. } 2 \quad \text{et} \quad t_n \equiv 6 \text{ mod. } 7 \quad \text{si } n \equiv 0 \text{ mod. } 2.$$

Puisque $n \geq 2$, on a $t_n \equiv 1$ mod. 4, d'où les égalités

$$\Big(\frac{t_n}{7}\Big) = \Big(\frac{7}{t_n}\Big) = -1,$$

et le critère d'Euler entraîne la congruence annoncée. Inversement, supposons que l'on ait $7^{\frac{t_n-1}{2}} \equiv -1$ mod. t_n. Posons

$$f_n = 2^{2^{n-1}}.$$

On a $t_n - 1 = f_n(f_n - 1)$ et $f_n \geq \sqrt{t_n}$. Par ailleurs, on a

$$7^{t_n-1} \equiv 1 \text{ mod. } t_n \quad \text{et} \quad 7^{\frac{t_n-1}{2}} - 1 \equiv -2 \text{ mod. } t_n.$$

La condition (23) est donc satisfaite pour t_n avec $a = 7$. Il en résulte que t_n est premier (th. 2.3), d'où l'équivalence (24). On vérifie avec ce critère que

$$t_6 = 18446744069414584321$$

est premier. Les entiers $n \leq 17$ tels que t_n soit premier sont $1, 2, 3$ et 6.

Brillhart, Lehmer et Selfridge ont démontré que l'on peut encore exploiter les conditions (22) et (23) avec des valeurs de F plus petites que $\sqrt{n}$, mais supérieures à $\sqrt[3]{n}$.

Théorème 2.4. *Supposons que les conditions* (22) *et* (23) *soient satisfaites et que l'on ait*

$$\sqrt[3]{n} \leq F < \sqrt{n}.$$

Il existe des entiers c_1 et c_2 tels que l'on ait

$$n = 1 + c_1F + c_2F^2 \quad \textit{avec} \quad 0 \leq c_i \leq F - 1. \tag{25}$$

Alors, n est premier si et seulement si $c_1^2 - 4c_2$ n'est pas un carré.

Démonstration : On a $n \equiv 1$ mod. F (assertion 1 du théorème 2.3). L'inégalité $\sqrt[3]{n} \leq F$ implique alors que l'écriture de n en base F est de la forme (25).

Supposons que n soit composé. D'après la première assertion du théorème 2.3 et l'inégalité $\sqrt[3]{n} \leq F$, chaque diviseur premier de n est plus grand strictement que $\sqrt[3]{n}$. Il en résulte que n est le produit de deux nombres premiers (éventuellement égaux). Posons

$$n = pq \quad \text{avec} \quad p = 1 + aF, \quad q = 1 + bF \quad \text{et} \quad a \leq b.$$

On a les égalités

$$n = 1 + c_1F + c_2F^2 = 1 + (a+b)F + abF^2. \tag{26}$$

Vérifions que l'on a

$$c_1 = a + b \quad \text{et} \quad c_2 = ab, \tag{27}$$

ce qui prouvera que $c_1^2 - 4c_2$ est un carré. On remarque pour cela que l'on a

$$abF^2 < n \leq F^3,$$

d'où l'inégalité

$$ab \leq F - 1. \tag{28}$$

Démontrons alors que l'on a

$$a + b \leq F - 1 \quad \text{ou bien} \quad (a, b) = (1, F-1).$$

Supposons $a+b \geq F$. Si $a \geq 2$, vu que $a \leq b$, on a $a+b \leq 2b \leq ab \leq F-1$ (inégalité (28)), d'où une contradiction. On a donc $a = 1$. D'après l'hypothèse faite, on a ainsi $b \geq F - 1$. Par ailleurs, on a $ab = b \leq F - 1$, d'où $b = F - 1$ et notre assertion.
Si $(a, b) = (1, F-1)$, on obtient $n = (1+F)\big(1 + (F-1)F\big) = F^3 + 1$, ce qui contredit l'inégalité $n \leq F^3$. Il en résulte que l'on a

$$a + b \leq F - 1. \tag{29}$$

Les entiers $a+b$ et ab étant positifs, les conditions (26), (28) et (29), ainsi que le caractère d'unicité de l'écriture de n en base F, impliquent alors les égalités (27).

Inversement, supposons que $c_1^2 - 4c_2$ soit un carré. Posons $c_1^2 - 4c_2 = u^2$. On a l'égalité

$$n = \Big(\frac{c_1 + u}{2}F + 1\Big)\Big(\frac{c_1 - u}{2}F + 1\Big).$$

On a $c_1 \equiv u \bmod. 2$ donc $\frac{c_1+u}{2}$ et $\frac{c_1-u}{2}$ sont des entiers. La condition $F < \sqrt{n}$ implique $c_2 \neq 0$; en effet, si $c_2 = 0$, on a $n \leq 1 + (F-1)F \leq F^2$. Par suite, on a $c_1^2 - u^2 > 0$, d'où

$|u| < c_1$, de sorte que cette décomposition de n n'est pas triviale, donc n est composé, d'où le résultat.

Remarque 2.7. L'hypothèse $F < \sqrt{n}$ a seulement été utilisée pour démontrer que si n est premier alors $c_1^2 - 4c_2$ n'est pas un carré.

6. Critère de primalité de Lucas-Lehmer

On va établir un critère de primalité pour les entiers n dans le cas où l'on connaît la décomposition de $n+1$ en facteurs premiers. Il a été obtenu par Lucas en 1878 et par Lehmer en 1930.

Définition 2.7 (Suite de Lucas). *Soit a un entier relatif. La suite d'entiers $(V_k)_{k\in\mathbb{N}}$ définie par les égalités*

$$V_0 = 2, \quad V_1 = a \quad \text{et} \quad V_{k+1} = aV_k - V_{k-1} \quad \text{pour tout } k \geq 1,$$

est appelée suite de Lucas associée à l'entier a.

Théorème 2.5 (Critère de Lucas-Lehmer). *Soit $n > 1$ un entier impair. Soient a un entier relatif et $(V_k)_{k\in\mathbb{N}}$ la suite de Lucas qui lui est associée. Supposons que les conditions suivantes soient satisfaites :*

1) on a $\operatorname{pgcd}(a^2 - 4, n) = 1$.

2) On a $V_{n+1} \equiv 2 \bmod n$.

3) Pour tout diviseur premier q de $n+1$, on a $\operatorname{pgcd}\left(V_{\frac{n+1}{q}} - 2, n\right) = 1$.

Alors, n est premier.

Afin de prouver cet énoncé, commençons par établir deux lemmes préliminaires. Soit p un nombre premier impair. Notons encore a la classe de a modulo p et considérons l'anneau quotient

$$A = \mathbb{F}_p[X]/(X^2 - aX + 1). \tag{30}$$

Identifions $\mathbb{F}_p$ à un sous-anneau de A. Soit α la classe de X modulo l'idéal $(X^2 - aX + 1)$. On a $\alpha^2 - a\alpha + 1 = 0$. En particulier, α est inversible dans A, et l'on a

$$\alpha + \alpha^{-1} = a. \tag{31}$$

Lemme 2.10. *Posons $\Delta = a^2 - 4$ et supposons que p ne divise pas Δ. On a*

$$\Delta^{\frac{p-1}{2}} \equiv \pm 1 \text{ mod. } p.$$

1) Si $\Delta^{\frac{p-1}{2}} \equiv 1$ mod. p, on a $\alpha^{p-1} = 1$. Si $\Delta^{\frac{p-1}{2}} \equiv -1$ mod. p, on a $\alpha^{p+1} = 1$.

2) Pour tout entier m, on a l'équivalence

$$\alpha^m = 1 \Longleftrightarrow \alpha^m + \alpha^{-m} = 2.$$

Démonstration : 1) Puisque p ne divise pas Δ, on a $\Delta^{p-1} \equiv 1$ mod. p, par suite, on a $\Delta^{\frac{p-1}{2}} \equiv \pm 1$ mod. p. On a l'égalité

$$(2\alpha - a)^2 = 4\alpha(\alpha - a) + a^2.$$

D'après (31), on obtient ainsi

$$(2\alpha - a)^2 = a^2 - 4 = \Delta + p\mathbb{Z}.$$

En élevant les deux membres de cette égalité à la puissance $\frac{p-1}{2}$, on obtient

$$(2\alpha - a)^{p-1} = \Delta^{\frac{p-1}{2}} + p\mathbb{Z}.$$

En posant $\varepsilon = \Delta^{\frac{p-1}{2}} + p\mathbb{Z}$, cela conduit à l'égalité

$$(2\alpha - a)^p = (2\alpha - a)\varepsilon.$$

Parce que A est de caractéristique p, on a $(2\alpha - a)^p = 2^p\alpha^p - a^p$. Par ailleurs, on a les congruences $2^p \equiv 2$ mod. p et $a^p \equiv a$ mod. p. On obtient ainsi

$$(2\alpha - a)\varepsilon = 2\alpha^p - a.$$

Si $\varepsilon = 1$, vu que 2 et α sont inversibles dans A (2 est inversible dans A, car A est un anneau de caractéristique non nulle $p \neq 2$), on obtient $\alpha^{p-1} = 1$. Si $\varepsilon = -1$, on a $2\alpha^p - a = a - 2\alpha$, d'où $2(\alpha^p + \alpha) = 2a$, puis $\alpha^p + \alpha = a$. L'égalité (31) entraîne alors la relation $\alpha^{p+1} = 1$, d'où la première assertion.

2) Vérifions d'abord que pour tout $x \in A$, l'égalité $x^2 = 0$ implique $x = 0$. Puisque $(1, \alpha)$ est une base du $\mathbb{F}_p$-espace vectoriel A, il existe u et v dans $\mathbb{F}_p$ tels que l'on ait $x = u + v\alpha$. On a

$$x^2 = u^2 - v^2 + (av^2 + 2uv)\alpha.$$

Dans $\mathbb{F}_p$, on obtient ainsi les égalités

$$(u - v)(u + v) = 0 \quad \text{et} \quad av^2 + 2uv = 0.$$

On a donc $u = \pm v$, puis $v^2(a \pm 2) = 0$. Par hypothèse, p ne divise pas $a^2 - 4$, autrement dit, $a + 2$ et $a - 2$ ne sont pas nuls dans $\mathbb{F}_p$, d'où $v = u = 0$ puis $x = 0$ et l'assertion.
Considérons alors un entier relatif m. Si $\alpha^m = 1$ il est immédiat que $\alpha^m + \alpha^{-m} = 2$. Inversement, si $\alpha^m + \alpha^{-m} = 2$, on a $(\alpha^m - 1)^2 = 0$. Compte tenu de ce qui précède, cela implique $\alpha^m = 1$, d'où le résultat.

Lemme 2.11. *Pour tout $k \in \mathbb{N}$, on a*

$$V_k + p\mathbb{Z} = \alpha^k + \alpha^{-k}.$$

Démonstration : Cette égalité est vraie si $k = 0$ et $k = 1$. Soit $k \geq 1$ un entier tel que pour tout $j \leq k$, on ait $V_j + p\mathbb{Z} = \alpha^j + \alpha^{-j}$. On a alors

$$V_{k+1} + p\mathbb{Z} = (aV_k - V_{k-1}) + p\mathbb{Z} = a(\alpha^k + \alpha^{-k}) - (\alpha^{k-1} + \alpha^{1-k}).$$

En utilisant (31), on obtient $V_{k+1} + p\mathbb{Z} = \alpha^{k+1} + \alpha^{-(k+1)}$ et l'assertion.

Démonstration du théorème : Soit p un diviseur premier de n. On considère l'anneau A associé à p défini par l'égalité (30) et l'élément $\alpha = X + (X^2 - aX + 1)$. D'après la condition 1, l'entier $a^2 - 4$ n'est pas divisible par p, et les conditions 2 et 3 impliquent

$$V_{n+1} \equiv 2 \text{ mod. } p \quad \text{et} \quad V_{\frac{n+1}{q}} \not\equiv 2 \text{ mod. } p, \tag{32}$$

pour tout diviseur premier q de $n + 1$.
D'après la seconde assertion du lemme 2.10, le lemme 2.11 et la condition (32), on obtient

$$\alpha^{n+1} = 1 \quad \text{et} \quad \alpha^{\frac{n+1}{q}} \neq 1,$$

pour tout diviseur premier q de $n+1$. Cela entraîne que α est d'ordre $n+1$ dans le groupe des éléments inversibles de A. Compte tenu de la première assertion du lemme 2.10, on a

$$\alpha^{p-1} = 1 \quad \text{ou} \quad \alpha^{p+1} = 1.$$

Par suite, $n+1$ divise $p \pm 1$. Le fait que l'on ait $p \leq n$ entraîne alors l'égalité $n + 1 = p + 1$ i.e. $n = p$, ce qui prouve que n est premier, d'où le résultat.

On en déduit un critère de primalité pour les nombres de Mersenne. Rappelons qu'il s'agit des entiers de la forme $2^p - 1$, où p est un nombre premier.

Proposition 2.8. *Soit $p \geq 3$ un nombre premier. Soit $(L_i)_{i \geq 1}$ la suite d'entiers définie par les égalités*

$$L_1 = 4 \quad \text{et} \quad L_{i+1} = L_i^2 - 2.$$

Supposons que l'on ait

$$L_{p-1} \equiv 0 \text{ mod. } 2^p - 1.$$

Alors, $2^p - 1$ *est premier.*

Établissons d'abord le lemme suivant :

Lemme 2.12. *Soient* a *un entier relatif et* $(V_k)_{k\in\mathbb{N}}$ *la suite de Lucas associée à l'entier* a*. Pour tout* $k \in \mathbb{N}$*, on a*

$$V_{2k} = V_k^2 - 2.$$

Démonstration : Soit t est un nombre complexe tel que $a = t + t^{-1}$. On vérifie par récurrence que l'on a $V_k = t^k + t^{-k}$ pour tout $k \in \mathbb{N}$. Cela implique l'égalité annoncée.

Démonstration de la proposition : Posons $n = 2^p - 1$. Soit $(V_k)_{k\in\mathbb{N}}$ la suite de Lucas associé à l'entier $a = 4$. D'après le lemme 2.12, pour tout $i \geq 1$ on a

$$V_{2^i} = V_{2^{i-1}}^2 - 2. \tag{33}$$

On en déduit l'égalité

$$L_i = V_{2^{i-1}}.$$

D'après l'hypothèse faite, on a donc

$$V_{2^{p-2}} \equiv 0 \text{ mod. } n.$$

En utilisant (33), on obtient les congruences

$$V_{\frac{n+1}{2}} = V_{2^{p-1}} \equiv -2 \text{ mod. } n \quad \text{et} \quad V_{n+1} \equiv 2 \text{ mod. } n.$$

Puisque p est impair, 12 est premier avec n. Le théorème 2.5 entraîne alors le résultat.

Remarque 2.8. La condition

$$L_{p-1} \equiv 0 \text{ mod. } 2^p - 1$$

caractérise en fait les nombres de Mersenne premiers (test de Lucas) ; si cette congruence n'est pas satisfaite, alors $2^p - 1$ est composé (exercice 17 du chapitre II).
On connaît cinquante et un nombres premiers de Mersenne,

$$2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31, \cdots 2^{19} - 1, \cdots 2^{61} - 1, \cdots$$

mais on ne sait pas prouver qu'il en existe une infinité. Par exemple, $2^{86243} - 1$ est premier. En utilisant le logiciel de calculs Pari, on peut le vérifier en trois minutes environ avec le test de Lucas. Il possède 25962 chiffres décimaux. De même, on peut vérifier que $2^{756839} - 1$ est premier, son nombre de chiffres décimaux est 227832 (le temps de calculs est de 5h30). Ce dernier a été découvert en février 1992. Le plus grand nombre premier aujourd'hui connu est un nombre de Mersenne. Il s'agit de

$$2^{82.589.933} - 1,$$

découvert en décembre 2018. Il possède 24862048 chiffres décimaux. On ne sait pas non plus démontrer l'existence d'une infinité de nombres premiers p tels que $2^p - 1$ soit composé.

7. Une variante du théorème d'Agrawal, Kayal et Saxena

En 2002, Agrawal, Kayal et Saxena ont établi un critère de primalité à temps de complexité polynomiale. Autrement dit, ils ont démontré que le nombre d'opérations arithmétiques pour prouver qu'un entier n est premier, si tel est le cas, peut s'effectuer en un $O\big((\log n)^k\big)$, où k est une constante positive. Le temps d'exécution d'un tel critère est donc borné par une puissance fixe du nombre de chiffres décimaux de n. Le point de départ repose sur le lemme suivant.

Lemme 2.13. *Soit $n \geq 2$ un entier. Soit a un entier relatif premier avec n. Alors, n est premier si et seulement si on a*

$$(X+a)^n \equiv X^n + a \text{ mod. } n\mathbb{Z}[X]. \tag{34}$$

Démonstration : La condition est nécessaire, car si n est premier, le coefficient binomial $\binom{n}{j}$ est divisible par n pour $j = 1, \cdots, n-1$ et $a^n \equiv a$ mod. n (que a soit premier avec n ou pas). Inversement, supposons la congruence (34) satisfaite. Puisque a et n sont premiers entre eux, on a

$$\binom{n}{i} \equiv 0 \text{ mod. } n \quad \text{pour} \quad i = 1, \cdots, n-1. \tag{35}$$

Vérifions que l'on a

$$\binom{n-1}{i} \equiv (-1)^i \text{ mod. } n \quad \text{pour} \quad i = 0, \cdots, n-1. \tag{36}$$

C'est vrai si $i = 0$. Soit i un entier tel que $0 \leq i \leq n-2$ et que (36) soit vraie pour i. On a

$$\binom{n-1}{i} + \binom{n-1}{i+1} = \binom{n}{i+1}.$$

On déduit de (35) la congruence

$$\binom{n-1}{i} \equiv -\binom{n-1}{i+1} \text{ mod. } n.$$

Cela entraîne notre assertion. Soit alors d un diviseur strict de n. D'après (35), on a

$$\binom{n}{d} = \frac{n}{d}\binom{n-1}{d-1} \equiv 0 \text{ mod. } n.$$

En utilisant (36) avec $i = d-1$, on obtient

$$\frac{n}{d}(-1)^{d-1} \equiv 0 \text{ mod. } n,$$

d'où $d = 1$ et le résultat.

Ce lemme fournit ainsi un critère de primalité. Son inconvénient est que l'on ne connaît pas de moyen rapide de vérifier la condition (34) vu le grand nombre de monômes de $(X+a)^n$. Il est donc inutilisable pratiquement. Cela étant, pour tout $F \in \mathbb{Z}[X]$, la condition (34) implique en particulier

$$(X + a)^n \equiv X^n + a \text{ mod. } (n, F), \tag{37}$$

où (n, F) est l'idéal de $\mathbb{Z}[X]$ engendré par n et F. Si n est premier, la congruence (37) doit donc être satisfaite. Si le degré de F n'est pas trop grand, il devient alors possible de la tester. Avec $a = 1$ et $F = X - 1$, elle signifie que l'on a

$$2^n \equiv 2 \text{ mod. } n.$$

Cette congruence n'est pas suffisante pour assurer que n est premier, de sorte que la condition (37) ne constitue pas un critère de primalité. Par exemple, on a

$$(X + 5)^{1729} \equiv X^{1729} + 5 \equiv X + 5 \text{ mod. } (1729, X^3 - 1),$$

or 1729 n'est pas premier. Agrawal, Kayal et Saxena ont néanmoins démontré que pour un entier r convenable, si la condition (37) est satisfaite avec $F = X^r - 1$ et suffisamment d'entiers a, alors n est une puissance d'un nombre premier. Plus précisément, en notant $\log_2 n$ le logarithme en base 2 de n :

Théorème 2.6 (Agrawal, Kayal, Saxena). *Soit $n \geq 2$ un entier. Soit r un entier naturel, premier avec n, tel que les conditions suivantes soient satisfaites :*

1) l'ordre multiplicatif de n modulo r est strictement plus grand que $(\log_2 n)^2$.

2) Les diviseurs premiers de n sont strictement plus grands que r.

3) On a la congruence

$$(X + a)^n \equiv X^n + a \text{ mod. } (n, X^r - 1) \quad \textit{pour tout } a \textit{ tel que} \quad 1 \leq a \leq \sqrt{r} \log_2 n. \tag{38}$$

Alors, n est une puissance d'un nombre premier.

Remarques 2.9.

1) Il existe un nombre premier r_0 pour lequel la première condition de l'énoncé est satisfaite. En posant

$$N = n(n-1)(n^2-1)\cdots(n^{[(\log_2 n)^2]} - 1),$$

il suffit de prendre pour r_0 le plus petit nombre premier qui ne divise pas N. On peut démontrer que le plus petit entier naturel r réalisant cette condition est inférieur à $(\log_2 n)^5$.

2) Étant donné un entier $n \geq 2$, si l'on sait que n est une puissance d'un nombre premier, il est facile de prouver que n est premier si tel est le cas. Il suffit de tester si $n^{\frac{1}{k}}$ n'est pas un entier, pour tout entier k compris entre 2 et $\log_2 n$, ce que l'on peut faire en calculant le nombre réel $n^{\frac{1}{k}}$ avec une précision suffisante. Si par exemple n n'est pas carré, on se limite à examiner les entiers k impairs.

Bien que le théorème 2.6 soit en temps d'exécution polynomial, et que cela soit un résultat théorique majeur, il reste aujourd'hui difficile à exploiter pratiquement. Afin d'essayer de le rendre performant d'un point de vue pratique, certaines variantes de ce théorème ont été établies. L'une d'entre elles permet d'éviter d'avoir à tester les congruences (38) pour tous les entiers plus petits que $\sqrt{r}\log_2 n$. Elle consiste essentiellement à tester une seule congruence, quitte à remplacer le polynôme $X^r - 1$ par $X^r - a$, où a est un entier convenable. Comme on le verra à travers des exemples, cette variante n'est pas encore compétitive par rapport à d'autres critères de primalité, mais de futures améliorations pourront peut-être y remédier. Il s'agit du résultat suivant démontré par Bernstein en 2003.

Théorème 2.7. *Soit $n \geq 2$ un entier. Soient a et r des entiers naturels vérifiant les conditions suivantes :*

1) on a $n \equiv 1$ mod. r et $r > (\log_2 n)^2$.

2) On a

$$a^{n-1} \equiv 1 \text{ mod. } n \quad \textit{et} \quad \operatorname{pgcd}\left(a^{\frac{n-1}{q}} - 1, n\right) = 1,$$

pour tout diviseur premier q de r.

3) On a la congruence

$$(X-1)^n \equiv X^n - 1 \ \text{ mod. } (n, X^r - a). \tag{39}$$

Alors, n est une puissance d'un nombre premier.

Démonstration : Soit p un diviseur premier de n. Il s'agit de prouver que n est une puissance de p. Posons

$$\overline{a} = a + p\mathbb{Z} \quad \text{et} \quad A = \mathbb{F}_p[X]/(X^r - \overline{a}).$$

Identifions $\mathbb{F}_p$ à un sous-anneau de A. Notons x la classe de X dans A. Posons

$$\alpha = \overline{a}^{\frac{n-1}{r}} \in \mathbb{F}_p.$$

L'élément α est d'ordre r dans $\mathbb{F}_p^*$. En effet, on a $\alpha^r = 1$ et pour tout diviseur premier q de r, on a

$$\alpha^{\frac{r}{q}} = \overline{a}^{\frac{n-1}{q}} \neq 1,$$

car p divise n et par hypothèse les entiers $a^{\frac{n-1}{q}} - 1$ et n sont premiers entre eux. En particulier,

$$r \text{ divise } p-1. \tag{40}$$

Vérifions que l'on a

$$(x-1)^{n^j} = \alpha^j x - 1 \quad \text{pour tout } j \in \mathbb{N}. \tag{41}$$

Dans A, on a $x^r = \overline{a}$, d'où les égalités

$$x^n = x.x^{n-1} = x(x^r)^{\frac{n-1}{r}} = x\overline{a}^{\frac{n-1}{r}} = \alpha x.$$

D'après (39), on a $(x-1)^n = x^n - 1$, d'où l'on déduit que

$$(x-1)^n = \alpha x - 1,$$

autrement dit, on a

$$(X-1)^n \equiv \alpha X - 1 \text{ mod. } (X^r - \overline{a}).$$

Puisque $\alpha^r = 1$, on a aussi

$$(\alpha^i X - 1)^n \equiv \alpha^{i+1} X - 1 \text{ mod. } (X^r - \overline{a}) \quad \text{pour tout } i \in \mathbb{N}. \tag{42}$$

La relation (41) est vraie si $j = 0$. Supposons qu'elle le soit pour un entier $j \in \mathbb{N}$. D'après (42), on obtient

$$(x-1)^{n^{j+1}} = (\alpha^j x - 1)^n = \alpha^{j+1} x - 1,$$

donc (41) est vraie pour l'entier $j+1$, d'où l'assertion.

Par ailleurs, on a

$$\left(a^{\frac{p-1}{r}}\right)^r = a^{p-1} \equiv 1 \text{ mod. } p.$$

D'après la condition (40), il existe un unique sous-groupe de $\mathbb{F}_p^*$ d'ordre r, à savoir celui engendré par α. Puisque $\overline{a}^{\frac{p-1}{r}}$ est dans ce sous-groupe, il existe $k \in \mathbb{N}$ tel que l'on ait $\overline{a}^{\frac{p-1}{r}} = \alpha^k$. On a ainsi

$$x^p = x.x^{p-1} = x(x^r)^{\frac{p-1}{r}} = x\overline{a}^{\frac{p-1}{r}} = \alpha^k x. \tag{43}$$

Vérifions alors que l'on a

$$(x-1)^{p^i(\frac{n}{p})^j} = \alpha^{j(1-k)+ik} x - 1 \quad \text{pour tous } i, j \in \mathbb{N}. \tag{44}$$

Soient i, j des entiers naturels. Vu que α^k est dans $\mathbb{F}_p$, on a

$$(\alpha^k)^p = \alpha^k.$$

Il résulte de (43) l'égalité

$$x^{p^i} = \alpha^{ik} x.$$

Compte tenu de (41), on obtient

$$(x-1)^{p^i n^j} = (\alpha^j x - 1)^{p^i} = \alpha^j x^{p^i} - 1 = \alpha^{j+ik} x - 1. \tag{45}$$

On passe de (44) à (45) en élevant les deux membres de (44) à la puissance p^j. Afin obtenir (44), tout revient donc à prouver que l'application $y \mapsto y^{p^j}$ est une bijection de A, autrement dit, que l'élévation à la puissance p est une bijection de A. Pour cela, on remarque que $X^r - \overline{a} \in \mathbb{F}_p[X]$ est séparable vu que p ne divise pas r. Par suite, A est un produit de corps finis de caractéristique p, et le théorème chinois entraîne alors notre assertion[3]. Cela établit (44).

Prouvons ensuite que $x - 1$ est un élément inversible de A. Il suffit de vérifier que $X - 1$ et $X^r - \overline{a}$ sont premiers entre eux dans $\mathbb{F}_p[X]$. On a la congruence

$$X^r - \overline{a} \equiv 1 - \overline{a} \text{ mod. } (X-1),$$

Puisque $\alpha = \overline{a}^{\frac{n-1}{r}}$ est d'ordre $r > 1$, on a $\overline{a} \neq 1$, d'où l'assertion.

Soit d l'ordre de $x - 1$ dans le groupe des éléments inversibles de A. Vérifions que l'on a

$$d \geq 2^r - 1. \tag{46}$$

Considérons pour cela les éléments

$$y_S = \prod_{j \in S} (\alpha^j x - 1),$$

où S parcourt les sous-ensembles stricts de $\{0, 1, \cdots, r-1\}$. On a

$$y_S \neq y_{S'} \quad \text{si} \quad S \neq S'.$$

En effet, parce que le système $(x^j)_{0 \leq j < r}$ est une base du $\mathbb{F}_p$-espace vectoriel A, cela revient à vérifier que l'on a dans $\mathbb{F}_p[X]$,

$$\prod_{j \in S} (\alpha^j X - 1) \neq \prod_{j \in S'} (\alpha^j X - 1) \quad \text{si} \quad S \neq S'.$$

[3] On utilise ici le fait que si K est un corps fini de caractéristique p, l'application de K^* dans K^* qui à z associe z^p est un morphisme injectif de groupes. Puisque K est fini, c'est un isomorphisme.

Tel est le cas, car α est d'ordre r, et si S est distinct de S' les polynômes ci-dessus n'ont donc pas les mêmes racines. Par ailleurs, il y a $2^r - 1$ sous-ensembles stricts de $\{0, 1, \cdots, r-1\}$. L'ensemble des éléments y_S est donc de cardinal $2^r - 1$. D'après l'égalité (41), chacun des y_S est une puissance de $x - 1$. Notons ces éléments

$$(x-1)^{N_1}, \cdots, (x-1)^{N_t} \quad \text{avec} \quad t = 2^r - 1.$$

Il existe des entiers q_i et h_i tels que l'on ait

$$N_i = dq_i + h_i \quad \text{avec} \quad 0 \leq h_i < d.$$

On obtient ainsi

$$(x-1)^{N_i} = (x-1)^{h_i} \quad \text{pour} \quad i = 1, \cdots, t.$$

Les éléments $(x-1)^{h_i}$ étant distincts deux à deux, il en est de même des h_i. Cela entraîne $t \leq d$, d'où l'inégalité (46).

Considérons alors l'ensemble des couples d'entiers (i, j) tels que

$$0 \leq i, j \leq \sqrt{r}. \tag{47}$$

Il y en a $([\sqrt{r}]+1)^2$ qui est $> r$. Par suite, il existe deux couples distincts (i_1, j_1) et (i_2, j_2) vérifiant la condition (47) tels que l'on ait

$$j_1(1-k) + i_1 k \equiv j_2(1-k) + i_2 k \text{ mod. } r.$$

Posons

$$u_1 = p^{i_1}\Big(\frac{n}{p}\Big)^{j_1} \quad \text{et} \quad u_2 = p^{i_2}\Big(\frac{n}{p}\Big)^{j_2}.$$

D'après l'égalité (44) et le fait que α soit d'ordre r, on obtient

$$(x-1)^{u_1} = \alpha^{j_1(1-k)+i_1 k} x - 1 = \alpha^{j_2(1-k)+i_2 k} x - 1 = (x-1)^{u_2}.$$

Puisque $x - 1$ est inversible, on a donc $(x-1)^{u_1 - u_2} = 1$, d'où

$$u_1 \equiv u_2 \text{ mod. } d.$$

D'après (47), on a

$$1 \leq u_1 \leq p^{\sqrt{r}}\Big(\frac{n}{p}\Big)^{\sqrt{r}} = n^{\sqrt{r}} \quad \text{et} \quad 1 \leq u_2 \leq n^{\sqrt{r}}.$$

Par ailleurs, en tenant compte de la condition

$$r > (\log_2 n)^2,$$

et de l'inégalité (46), on a

$$n^{\sqrt{r}} < d + 1.$$

On obtient

$$1 \leq u_1, u_2 \leq d.$$

Il en résulte que l'on a $u_1 = u_2$. On en déduit l'égalité

$$p^{i_1+j_2} n^{j_1} = p^{i_2+j_1} n^{j_2}.$$

S'il existe un nombre premier distinct de p qui divise n, on obtient alors $j_1 = j_2$, puis $i_1 = i_2$, ce qui contredit le fait que les couples (i_1, j_1) et (i_2, j_2) soient distincts. Par suite, n est une puissance de p. Cela termine la démonstration du théorème.

Remarque 2.10. Avec les notations du théorème 2.7, On a

$$X^n = X\big(X^r\big)^{\frac{n-1}{r}} \equiv a^{\frac{n-1}{r}} X \text{ mod. } (X^r - a) \tag{48}$$

de sorte que le calcul de X^n modulo l'idéal $(n, X^r - a)$ se réduit à celui de $a^{\frac{n-1}{r}}$ modulo n, ce qui est immédiat.

Exemples 2.10.

1) Prenons $n = 2^{116} - 3$, qui a trente-cinq chiffres décimaux. On a $(\log_2 n)^2 \simeq 13456$ et l'on vérifie que

$$r = 4 \times 7 \times 571 = 15988$$

divise $n - 1$. Par ailleurs, la condition 2 du théorème 2.7 est satisfaite avec $a = 2$. On constate, en quelques secondes avec le logiciel de calculs Pari, que l'on a

$$(X - 1)^n \equiv 2^{\frac{n-1}{r}} X - 1 \text{ mod. } (n, X^r - 2),$$

ce qui, compte tenu de (48), prouve que n est une puissance d'un nombre premier. On vérifie ensuite que n est premier (seconde remarque 2.9).

2) Prenons $n = 2^{150} - 3$. Il a quarante-six chiffres décimaux. On a $(\log_2 n)^2 \simeq 22500$. L'entier

$$r = 3 \times 5 \times 1777 = 26655$$

divise $n - 1$. En vingt secondes environ sur Pari, on obtient la même congruence que celle ci-dessus, ce qui permet d'établir que n est premier.

Remarque 2.11. Comme on l'a signalé, on dispose de méthodes beaucoup plus rapides pour établir que ces entiers sont premiers, par exemple le test de Pocklington. Pour $n = 2^{116} - 3$, on a

$$n - 1 \equiv 0 \text{ mod. } F \quad \text{avec} \quad F = 2^2 \times 3^2 \times 7 \times 571 \times 32377 \times 174763 \times 524287.$$

On obtient facilement cette congruence en recherchant les petits diviseurs premiers de $n - 1$. La condition (23) du théorème 2.3 est satisfaite avec $a = 2$ et l'entier F. Puisque F est plus grand que $\sqrt{n}$, cela prouve que n est premier.