L'algorithme $\mathcal{AKS}$
ou
Les nombres premiers sont de classe $\mathcal{P}$

Julien Élie*

« Le plus beau résultat mathématique des dix dernières années. »

Shafi Goldwasser

En août 2002, le professeur $\mathcal{A}$grawal et deux de ses élèves, $\mathcal{K}$ayal et $\mathcal{S}$axena, résolvent une ancienne conjecture en théorie de la complexité : le test en temps polynomial de la primarité d'un nombre donné.

Dans cet exposé, je m'intéresse à la seconde version parue en mars 2003 de l'algorithme $\mathcal{AKS}$ et me propose de démontrer intégralement sa validité. La démonstration est entièrement accessible et ne repose sur aucune hypothèse.

« Le problème où l'on se propose de distinguer les nombres premiers des nombres composés, et de résoudre ceux-ci en leurs facteurs premiers, est connu comme l'un des plus importants et des plus utiles de toute l'Arithmétique ; il a sollicité l'industrie et la sagacité des géomètres tant anciens que modernes, à un point tel qu'il serait superflu de discuter en détail à cet égard. [...]

« De surcroît, la dignité de la science même semble demander que tous les secours possibles soient explorés avec soin pour parvenir à la solution d'un problème si élégant et si célèbre. »

Johann Carl Friedrich Gauss, *Disquisitiones Arithmeticæ*, 329.

*D'après un TIPE rédigé en 2003 avec $\mathcal{AMS}$-LaTeX 2$_\varepsilon$ sous la direction de MM. Serge Francinou et Philippe Espéret, professeurs de mathématiques au Lycée Henri-IV de Paris.

Table des matières

1 Introduction

1.1 Intérêt de l'algorithme

Les nombres premiers jouent un rôle fondamental en mathématiques et possèdent moult applications très utiles de nos jours, notamment dans le domaine de la cryptographie. Il est donc intéressant d'établir des tests pratiques et fiables de primarité.

Depuis l'invention de la théorie de la complexité dans les années 1960, le problème que nous noterons $\mathscr{P}$, qui est de savoir si un nombre donné n est premier, passionne les chercheurs.

Le tableau ci-dessous dresse la liste chronologique des algorithmes majeurs qui ont été trouvés afin de déterminer la primarité d'un nombre.

Algorithme :	Année :	D.[a] :	P.[b] :	I.[c] :	Principe :
Crible d'Ératosthène	≈ -240	✓	✗	✓	Division de n par tous les nombres (premiers) $\leqslant \sqrt{n}$
Miller	1975	✓	✓	✗	Recherche de témoins de non-primarité[d]
Rabin	1976	✗	✓	✓	
Solovay et Strassen	1977	✗	✓	✓	Résidus quadratiques[e] : test de $a^{\frac{n-1}{2}} = (\frac{a}{n})\ [n]$ pour plusieurs $a \in \mathbb{N}$
		✓	✓	✗	
Adleman, Pomerance et Rumely	1983	✓	✗	✓	Test de primarité[f] (d'après Miller) à base de réciprocité quadratique
Goldwasser et Kilian Atkin	1986	✗	✗	✓	Courbes elliptiques
			✓	✗	
Adleman et Huang	1992	✗	✓	✓	Courbes hyperelliptiques
Agrawal, Kayal et Saxena	2002	✓	✓	✓	Polynômes cyclotomiques sur des corps finis — en $\Omega(\log(n)^{10.5})$

Tab. 1 – Principaux algorithmes de primarité.

[a] $\mathcal{D}$éterministe.
[b] $\mathcal{P}$olynomial.
[c] $\mathcal{I}$nconditionnel : l'hypothèse de Riemann généralisée est utilisée pour les algorithmes ne satisfaisant pas ce critère.
[d] Si $n-1 = 2^s t$ avec t impair et s'il existe $1 < a < n$ tel que $a^t \not\equiv 1\ [n]$ et $\begin{cases} a^{2^i t} \not\equiv -1 \quad [n] \\ 0 \leqslant i \leqslant s-1 \end{cases}$ alors n est composé. L'algorithme est en $O(\log(n)^2)$.
[e] $(\frac{a}{p}) = \begin{cases} 1 \text{ si } a \text{ carré dans } \mathbb{Z}/p\mathbb{Z} \\ -1 \text{ sinon} \end{cases}$ est le symbole de Jacobi.
[f] Complexité quasi polynomiale en $O(\log(n)^{O(\log(\log(\log(n))))})$.

Bien que des progrès aient été réalisés au fil des années, seul le dernier algorithme vérifie en même temps les trois critères présentés et qui sont détaillés *infra*.

Tout entier n composé possède une preuve très courte de non-primarité, à savoir un diviseur non trivial. Alors qu'il est très difficile d'exhiber les facteurs premiers des grands nombres, il est assez aisé de vérifier qu'un certain nombre en est bien un facteur premier : on dit alors que $\mathscr{P} \in$ co-$\mathcal{NP}$ où $\mathcal{NP}$ désigne la classe des problèmes qui peuvent être résolus en temps polynomial par un algorithme non déterministe (il suffit en effet de simplement effectuer la division avec le facteur magiquement exhibé), le préfixe « co » signifiant que c'est le problème complémentaire de composition des nombres qui est considéré. De plus, pour peu que l'on connaisse la décomposition en facteurs premiers de $n-1$, un critère de Lehmer énonce que si, pour un entier a, $a^{n-1} \equiv 1\ [n]$ et $a^{\frac{n-1}{q}} \not\equiv 1\ [n]$ pour tout diviseur premier q de $n-1$, alors n est premier, ce qui montre que $\mathscr{P} \in \mathcal{NP}$.

Or, les mathématiciens souhaiteraient aller plus loin et prouver que $\mathscr{P} \in \mathcal{P}$, où $\mathcal{P}$ désigne la classe des problèmes décisionnels, c'est-à-dire auxquels l'on peut répondre par « oui » ou par « non », qui peuvent être résolus par un algorithme déterministe en temps polynomial quel que soit l'argument n du problème.

L'algorithme $\mathcal{AKS}$ est la preuve cherchée, ce qui établit le résultat fondamental :

$$\mathscr{P} \in \mathcal{P}.$$

Et c'est ce problème de longue date qui vient d'être résolu en août 2002 par le professeur Manindra AGRAWAL et deux de ses élèves, Neeraj KAYAL et Nitin SAXENA, qui viennent d'obtenir leur licence dans le Département d'Informatique de l'*Institut Indien de Technologie* à Kanpur. Une seconde version améliorée de cet algorithme *« brillant, élégant et simple »* a ensuite été présentée en mars 2003. Cette nouvelle version est plus élégante et ne requiert pas de résultats pointus d'algèbre afin d'être démontrée dans son intégralité.

Par ailleurs, un intérêt non négligeable de l'algorithme $\mathcal{AKS}$ est qu'il ne nécessite que quelques outils assez simples d'algèbre afin d'être démontré, ce qui est loin d'être le cas pour les autres algorithmes de primarité qui font appel à des résultats très pointus en théorie des nombres.

L'importance du résultat présenté dans cet exposé est que l'algorithme $\mathcal{AKS}$ garantit l'obtention en un temps polynomial d'une réponse catégorique sur la primarité d'un nombre. De fait, cet algorithme se démarque de tous les autres puisqu'il réunit les trois critères fondamentaux que nous allons maintenant préciser plus en détail.

1.2 Un algorithme déterministe

L'algorithme $\mathcal{AKS}$ est déterministe, en ce sens qu'il détermine toujours pas un « oui » ou par un « non » définitif et sans erreur possible la primarité de l'entier donné. Mais il est plus facile de définir ce qu'est un algorithme déterministe par la négation de la nature d'un algorithme probabiliste.

Celui-ci peut faire partie de deux types :
- les **tests de composition** qui permettent de déterminer de manière sûre si un nombre est composé, sans pourtant nécessairement en fournir une décomposition explicite ;
- les **tests de primarité**, nettement moins rapides, qui permettent de déterminer de manière sûre si un nombre est premier.

Lorsque le test ne retourne pas une réponse catégorique, la probabilité de primarité ou de non-primarité du nombre est d'autant plus élevée que l'algorithme effectue d'itérations. Par exemple, pour le test de SOLOVAY-STRASSEN, il est démontré qu'il existe un entier a premier avec n sur deux qui ne vérifie pas le test ; aussi, en réitérant k fois l'algorithme avec des entiers a différents choisis au hasard, la probabilité d'erreur sur la primarité de n est-elle de l'ordre de $1/2^k$, s'il satisfait à chacun de ces tests, que l'on admettra indépendants. Ainsi, pour 50 itérations de ce test, le risque d'erreur est inférieur à 10^{-15}.

En pratique, les tests probabilistes de primarité actuels ont une probabilité d'erreur inférieure, dit-on, à la probabilité que le système informatique qui réalise le test commette une erreur tandis que dans la même minute son utilisateur remporte la cagnotte à la loterie et meure foudroyé ! Nonobstant, l'erreur est toujours *en théorie* possible, si bien que les mathématiciens essaient depuis de nombreuses années de la supprimer.

En outre, les algorithmes probabilistes utilisent des séquences de tests aléatoires à chaque utilisation, de telle sorte que des réponses différentes peuvent survenir lors du test du même nombre, ou l'algorithme peut tout simplement ne pas aboutir. Au contraire, un algorithme déterministe produira toujours *la même séquence d'opérations* pour le même argument fourni.

1.3 Un algorithme en temps polynomial

L'algorithme $\mathcal{AKS}$ donne une réponse en temps polynomial, en ce sens qu'il existe un polynôme P tel que, pour tout entier n, l'algorithme exécute au plus $P(\log(n))$ opérations élémentaires pour fournir le résultat, lorsque la donnée initiale est le nombre n. On convient que si $n = 0$, $P \equiv 0$. La complexité temporelle de l'algorithme est donc une fonction polynomiale en le nombre de chiffres nécessaires à représenter n, que ce soit $log_{10}(n)$ en base décimale ou $log_2(n)$ en base binaire.

À l'ère des micro-ordinateurs, de tels algorithmes sont considérés comme implémentables, à la différence des algorithmes en temps exponentiel inutilisables en pratique, puisque le temps de calcul devient rapidement trop important lorsque le nombre à tester devient grand.

Bien qu'il soit facile de prouver la complexité temporelle de l'algorithme $\mathcal{AKS}$ en $\Omega(\log(n)^{10.5})$, il est aussi possible de trouver une meilleure complexité en $\Omega(\log(n)^{7.5})$ grâce à des résultats de théorie des nombres.

Toutefois, cela reste encore assez lent étant donné que l'on estime que les algorithmes réellement utilisables doivent être au plus en $\Omega(\log(n)^3)$.

Cela n'a cependant aucune incidence sur le résultat théorique $\mathscr{P} \in \mathcal{P}$.

1.4 Un algorithme inconditionnel

L'algorithme $\mathcal{AKS}$ ne repose sur aucune hypothèse : sa validité, tout comme sa complexité temporelle polynomiale, sont entièrement prouvées et ne font pas appel à des conjectures de théorie des nombres, à la différence de la majorité des autres tests de primarité. Notons toutefois que si l'hypothèse de Riemann généralisée[1] était démontrée, on aurait déjà prouvé avec l'algorithme de Miller-Rabin en temps $O(\log(n)^2)$ que $\mathscr{P} \in \mathcal{P}$, mais le fait est que cette conjecture n'a toujours pas été prouvée.

2 Idée et description de l'algorithme

2.1 Identité remarquable

Le test de primarité $\mathcal{AKS}$ est fondé sur l'identité suivante, valable pour les nombres premiers, et qui est une généralisation du petit théorème de Fermat.

Proposition 2.1. *Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}$, $n \geqslant 2$, tels que $a \wedge n = 1$.*

$$n \text{ est premier si, et seulement si, } (X+a)^n \equiv X^n + a \quad [n].$$

Démonstration : Supposons n premier.

Pour tout $i \in [\![1, n-1]\!]$, $i\,C_n^i = n\,C_{n-1}^{i-1}$ donc n divise $i\,C_n^i$.

Comme n est premier avec i, n divise C_n^i en vertu du théorème de Gauss. Or, le coefficient de X^i dans le polynôme $(X+a)^n$ étant $C_n^i\,a^{n-i}$, il se retrouve divisible par n, si bien que $(X+a)^n \equiv X^n + a\ [n]$.

Réciproquement, supposons que l'on ait $(X+a)^n \equiv X^n + a\ [n]$.

Soit d une partie aliquote de n, autrement dit un diviseur strict de n : $1 \leqslant d < n$. On a : $C_n^d = \frac{n}{d}\,C_{n-1}^{d-1} \equiv 0\ [n]$ d'après l'identité puisque a est premier avec n.

Regardons les résidus des C_{n-1}^i modulo n.

Pour $i = 1$, $C_{n-1}^1 = n - 1 \equiv -1\ [n]$. Or, d'après la formule de Pascal, $C_{n-1}^i + C_{n-1}^{i+1} = C_n^{i+1}$, donc $C_{n-1}^{i+1} \equiv -\,C_{n-1}^i\ [n]$. Il s'ensuit par une récurrence immédiate que $C_{n-1}^i \equiv (-1)^i\ [n]$ pour tout $1 \leqslant i \leqslant n-1$, et $\frac{n}{d}\,C_{n-1}^{d-1} \equiv \frac{n}{d}\,(-1)^{d-1} \equiv 0\ [n]$, ce qui n'est possible que si $d = 1$.

Donc n est premier. □

[1] Cette conjecture sera énoncée au paragraphe 4.2.1.

Cette identité fournit donc un critère très simple de primarité : étant donné un nombre n, il suffit de choisir un entier a premier avec n puis de vérifier si la congruence est satisfaite. Cependant[2], cela prend un temps en $O(n)$ puisqu'il s'agit d'évaluer n coefficients dans le pire des cas.

Un moyen simple de réduire le nombre de coefficients est d'évaluer les deux membres de la congruence modulo un polynôme de la forme $X^r - 1$ pour un entier r plus petit que n bien choisi. En d'autres termes, il s'agit de vérifier si la congruence $(X + a)^n \equiv X^n + a$ est vraie dans l'anneau $\frac{\mathbb{Z}/n\mathbb{Z}[X]}{(X^r-1)\,\mathbb{Z}/n\mathbb{Z}[X]}$.

Mieux, si un tel r est choisi d'un ordre logarithmique en n, le polynôme résiduel peut être directement calculé en temps polynomial avec un algorithme approprié.

D'après la proposition précédente, il est immédiat de constater que tous les nombres n premiers satisfont cette équation pour tout a et pour tout r. Le problème est qu'il existe aussi des nombres composés qui vérifient l'équation pour quelques valeurs de a et de r. Par exemple, le troisième nombre de Carmichael[3], $n = 1729 = 7 \cdot 13 \cdot 19$, vérifie la congruence avec $a = 5$ et $r = 3$.

```
> Powmod(X + 5, 1729, X^3 - 1, X) mod 1729;
```

$$X + 5$$

```
> Powmod(X, 1729, X^3 - 1, X) + 5 mod 1729;
```

$$X + 5$$

Or, comme Carl Pomerance le fit plus tard remarquer à juste titre – « it seems a shame to give up on it just because there are a few counter examples » –, il fallait quand même persister dans cette direction ; si bien qu'il est possible d'utiliser cette caractérisation en montrant que l'on peut trouver un nombre r tel que si l'équation est vérifiée pour plusieurs nombres a déterminés, alors n est premier.

Cette découverte fut réalisée le 10 juillet 2002 : en fixant un r judicieux et en faisant varier a, naît une caractérisation des nombres premiers.

Toujours avec le même exemple, la congruence n'est effectivement plus vérifiée avec $r = 5$.

```
> Powmod(X + 5, 1729, X^5 - 1, X) mod 1729;
```

$$1254\ X^4 + 799\ X^3 + 556\ X^2 + 1064\ X + 1520$$

```
> Powmod(X, 1729, X^5 - 1, X) + 5 mod 1729;
```

$$X^4 + 5$$

La recherche de r et le nombre de vérifications à accomplir ensuite avec les a déterminés s'effectuent en un temps polynomial en $\log(n)$, si bien que l'on obtient effectivement un algorithme déterministe en temps polynomial pour des tests de primarité.

[2] D'ailleurs, si les créateurs de l'algorithme $\mathcal{AKS}$ en étaient restés là, celui-ci n'aurait été qu'un post-scriptum dans l'histoire des tests de primarité.

[3] De tels nombres, dont les deux premiers sont 561 et 1105, sont des entiers n non premiers tels que, pour tout a premier avec n, $a^{n-1} \equiv 1\ [n]$. En 1994, a été prouvée la conjecture qu'il existe une infinité de nombres de Carmichael.

2.2 L'algorithme $\mathcal{AKS}$

Nous sommes maintenant en mesure d'énoncer l'algorithme $\mathcal{AKS}$ en pseudo-code.

Soit un entier $n > 1$ donné.

1. Si $n = a^b$ pour $a \in \mathbb{N}$ et $b > 1$, alors n est Composé.
2. Déterminer le plus petit entier r tel que l'ordre de n dans $\mathbb{Z}/r\mathbb{Z}$ soit supérieur à $4\log(n)^2$.
3. Si $1 < a \wedge n < n$ pour un entier $a \leqslant r$, alors n est Composé.
4. Si $n \leqslant r$, alors n est Premier.
5. Pour $a = 1$ à $\left\lfloor 2\sqrt{\varphi(r)}\,\log(n) \right\rfloor$:
   si $(X+a)^n \not\equiv X^n + a$ dans $\frac{\mathbb{Z}/n\mathbb{Z}[X]}{(X^r-1)\mathbb{Z}/n\mathbb{Z}[X]}$, alors n est Composé.
6. n est Premier.

---

3 Validité de l'algorithme

3.1 Notations

Commençons par introduire quelques notations qui seront utilisées dans la suite de l'exposé.

Si p est premier, $\mathbb{F}_p$ désigne le *corps premier fini* à p éléments $\mathbb{Z}/p\mathbb{Z}$. Rappelons que si p est premier et si Q est un polynôme de degré d et irréductible sur $\mathbb{F}_p$, alors $\mathbb{F}_p/Q\mathbb{F}_p[X]$ est un $\mathbb{F}_p$-espace vectoriel de dimension d ; c'est même un corps fini de cardinal p^d car isomorphe en tant qu'espace vectoriel à $(\mathbb{F}_p)^d$.

Si P, Q et R sont des polynômes, on utilisera la notation $P(X) \equiv Q(X)\ [R(X),\ n]$ pour représenter la congruence $P(X) \equiv Q(X)$ dans l'anneau $\frac{\mathbb{Z}/n\mathbb{Z}[X]}{R\mathbb{Z}/n\mathbb{Z}[X]}$.

Si $r \in \mathbb{N}$ et $a \in \mathbb{Z}$ avec a et r premiers entre eux, l'*ordre* de a dans $(\mathbb{Z}/r\mathbb{Z})^\star$ est le plus petit entier k tel que $a^k \equiv 1\ [r]$. On notera alors $k = \omega_r(a)$.

Si $r \in \mathbb{N}$, $\varphi(r)$ est le nombre d'entiers inférieurs à r qui sont premiers avec r : φ désigne alors l'indicateur d'Euler.

Si p est premier et $n \in \mathbb{N}$, $\nu_p(n)$ désigne la *valuation p-adique* de n, à savoir l'exposant de p dans la décomposition en facteurs premiers de n.

Si $x \in \mathbb{R}$, on notera $\lfloor x \rfloor$ et $\lceil x \rceil$ la partie entière de x respectivement par défaut et par excès.

Sauf mention explicite du contraire en indice, le logarithme, noté « log », est celui de base 2.

3.2 Résultats liminaires

3.2.1 Un peu de dénombrement

Lemme 3.1. *Si $k \geqslant 3$, $C^k_{2k-1} \geqslant 2^k$.*

Preuve : Montrons le résultat par récurrence sur $k \geqslant 3$.

Si $k = 3$, on a bien $C_5^3 = 10 \geqslant 8 = 2^3$.

Soit $k \geqslant 4$.

$$C_{2(k+1)-1}^{k+1} = \frac{(2k+1)!}{(k+1)!\,k!} = \frac{(2k-1)!}{k!\,(k-1)!} \cdot \frac{2k}{k} \cdot \underbrace{\frac{2k+1}{k+1}}_{\geqslant 1} \geqslant 2\,C_{2k-1}^{k} \geqslant 2^{k+1} \quad \text{par hypothèse de récurrence.}$$

D'où le résultat. □

Lemme 3.2. *Soient $n, p \in \mathbb{N}^*$, $p \leqslant n$.*

$$C_n^p + C_{n-1}^p + \cdots + C_p^p = C_{n+1}^{p+1}.$$

Preuve : Établissons le résultat par récurrence sur n.

Si $n = 1$, alors $p = 1$ aussi et $C_1^1 = 1 = C_2^2$ donc la propriété est vérifiée.

Soit $n \geqslant 2$.

Si $p < n$, alors $C_{n+1}^{p+1} = C_n^p + C_n^{p+1} = C_n^p + C_{n-1}^p + C_{n-2}^p + \cdots + C_p^p$ en utilisant la relation de Pascal puis l'hypothèse de récurrence avec $p + 1 \leqslant n$.

Et si $n = p$, $C_{n+1}^{p+1} = 1 = C_n^p$.

La propriété est donc bien vérifiée. □

Lemme 3.3. *Soit $p \in \mathbb{N}$. Il existe C_{n+p-1}^n possibilités de choisir n entiers naturels dont la somme est inférieure ou égale à $p - 1$.*

Preuve : Soit $p \in \mathbb{N}^*$ fixé. Montrons le résultat par récurrence sur $n \in \mathbb{N}^*$.

Si $n = 1$, il y a p choix possibles. C'est bien $C_p^1 = p$.

Soit $n \geqslant 2$. Notons les n nombres considérés $\{e_i\}_{1 \leqslant i \leqslant n}$.

À e_n fixé, et si l'on tient compte de ce que $\sum_{i=1}^{n} e_i \leqslant p - 1$, choisissons les $n - 1$ nombres $\{e_i\}_{1 \leqslant i \leqslant n-1}$. Par hypothèse de récurrence, on a C_{n+p-2}^{n-1} possibilités si $e_n = 0$, C_{n+p-3}^{n-1} possibilités si $e_n = 1$, … et C_{n-1}^{n-1} possibilité si $e_n = p - 1$.

Cela fait donc $C_{n+p-2}^{n-1} + C_{n+p-3}^{n-1} + \cdots + C_{n-1}^{n-1} = C_{n+p-1}^{n}$ possibilités au total pour le choix des n entiers d'après le lemme 3.2 précédent.

D'où le résultat. □

3.2.2 Théorème d'Euler

Théorème 3.1. *Soient $a, n \in \mathbb{N}^*$. Si $a \wedge n = 1$, alors :*

$$a^{\varphi(n)} \equiv 1\ [n].$$

En particulier, $\omega_n(a) \mid \varphi(n)$.

(Théorème d'Euler — 1760)

Démonstration : Notons $k = \varphi(n)$ et considérons l'ensemble $r_1 < r_2 < \cdots < r_k$ des nombres naturels $r \leqslant n$ premiers avec n.

L'ensemble $\{ar_1, ar_2, \ldots, ar_k\}$ est une permutation des nombres $r_1, \ldots, r_k$ modulo n. En effet, si $1 \leqslant i, j \leqslant k$, comme $ar_i \wedge n = 1$, le reste de ar_i modulo n est l'un des nombres $r_1, \ldots, r_k$. Par ailleurs, $ar_i \equiv ar_j\ [n]$ implique $r_i \equiv r_j\ [n]$ en vertu du théorème de Gauss. Donc $r_i = r_j$.

Il s'ensuit que $(ar_1)(ar_2) \cdots (ar_k) \equiv r_1 r_2 \cdots r_k\ [n]$. Et comme n est premier avec $r_1 r_2 \cdots r_k$, il vient $a^k \equiv 1\ [n]$. D'où[4] $a^{\varphi(n)} \equiv 1\ [n]$.

Par définition de l'ordre de a modulo n, on a bien $\omega_n(a) \mid \varphi(n)$. □

[4]Cette relation est aussi une conséquence directe du théorème du comte de Lagrange appliqué à l'élément a modulo n puisque le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\star$ est $\varphi(n)$.

3.2.3 Introspection

Définition 3.1. *Soit K un anneau, $P \in K[X]$ et $n, p, r \in \mathbb{N}$, p premier.*
*On dit que n est **introspectif** pour P si $P(X)^n \equiv P(X^n) \quad [X^r - 1,\ p]$.*

L'ensemble des nombres introspectifs pour un polynôme donné dans $\frac{\mathbb{F}_p[X]}{(X^r-1)\mathbb{F}_p[X]}$ forme en fait un monoïde multiplicatif :

Lemme 3.4. *Si n et n' sont introspectifs pour un polynôme P, alors $n \cdot n'$ l'est aussi.*

Preuve : Puisque n est introspectif pour P, on a :

$$P(X)^{nn'} \equiv P(X^n)^{n'} \quad [X^r - 1,\ p].$$

Et comme n' est aussi introspectif pour P, on obtient en substituant X^m à X dans l'équation :

$$\begin{aligned} P(X^n)^{n'} &\equiv P(X^{nn'}) \quad [X^{nr} - 1,\ p] \\ &\equiv P(X^{nn'}) \quad [X^r - 1,\ p] \quad \text{car } X^r - 1 \mid X^{nr} - 1. \end{aligned}$$

En combinant les deux relations, il vient :

$$P(X)^{nn'} \equiv P(X^{nn'}) \quad [X^r - 1,\ p].$$

□

Pour un nombre n donné, l'ensemble des polynômes pour lesquels n est instrospectif dans $\frac{\mathbb{F}_p[X]}{(X^r-1)\mathbb{F}_p[X]}$ forme aussi un monoïde multiplicatif :

Lemme 3.5. *Si n est introspectif pour deux polynômes P et Q, alors n est aussi introspectif pour le produit PQ.*

Preuve : $(PQ)(X)^n = (P(X) \cdot Q(X))^n = P(X)^n \cdot Q(X)^n$.
D'où $(PQ)(X)^n \equiv P(X^n) \cdot Q(X^n) \equiv (PQ)(X^n) \quad [X^r - 1,\ p]$. □

3.3 Résultats préliminaires

3.3.1 Minoration du ppcm

Lemme 3.6. *Soit $m \in \mathbb{N}$, $m \geqslant 4$. Alors : $m\, C_{2m}^m \geqslant 4^m$.*

Preuve : Montrons le résultat par récurrence sur m.
Si $m = 4$, on a bien $4\, C_8^4 = 280 \geqslant 4^4 = 256$.
Supposons $m \geqslant 5$.
$(m+1)\, C_{2(m+1)}^{m+1} = \frac{(m+1)(2m+2)!}{(m+1)!\,(m+1)!} = \frac{(m+1)(2m)!\,(2m+1)(2m+2)}{m!\,m!\,(m+1)(m+1)} = 2(2m+1)\, C_{2m}^m \geqslant 4m\, C_{2m}^m \geqslant 4 \cdot 4^m = 4^{m+1}$ par hypothèse de récurrence.
Donc pour tout $m \geqslant 4$, $m\, C_{2m}^m \geqslant 4^m$. □

Lemme 3.7. *Soient $n \in \mathbb{N}$, $n \geqslant 2$ et p premier.*

$$\nu_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Preuve : Remarquons avant toute chose que la somme est bien définie puisqu'elle est à support fini. En effet, comme $p \geqslant 2$, il existe $k_0 \in \mathbb{N}$ tel que si $k \geqslant k_0$, $p^k > n$. Dans ces conditions, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ si $k \geqslant k_0$.

Dénombrons les multiples de p^k $(k \geqslant 1)$ parmi les entiers de 1 à n : le nombre de multiples de p^k qui ne sont pas multiples de p^{k+1} est $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$. Chacun de ces multiples apporte une contribution de k dans la valuation p-adique de $n!$.

D'où :

$$\nu_p(n!) = \sum_{k \geqslant 1} k \cdot \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

□

Proposition 3.1. *Soit $n \in \mathbb{N}$, $n \geqslant 7$. Alors le plus petit commun multiple des n premiers entiers naturels non nuls est supérieur ou égal à 2^n :*

$$\bigvee_{i=1}^{n} i \geqslant 2^n.$$

Démonstration : Notons $\psi : n \longmapsto \bigvee_{i=1}^{n} i$.

Remarquons tout d'abord que si n est impair, alors :

- soit $n+1$ est une puissance de 2, d'où $\psi(n+1) = 2\,\psi(n)$ puisque l'on rajoute une puissance de 2 supplémentaire jusques alors inexistante dans le plus petit commun multiple des n premiers entiers ;
- soit $n+1$ n'est pas une puissance de 2, d'où $\psi(n+1) = \psi(n)$.

Par suite, on a dans tous les cas $\psi(n) \geqslant \frac{1}{2}\,\psi(n+1)$, ce qui prouve que si l'inégalité est vraie pour $n+1$, alors elle l'est aussi pour n. Il suffit donc de prouver le résultat pour les entiers pairs supérieurs ou égaux à 8.

Montrons que pour tout entier $m \geqslant 1$, $m\,C_{2m}^m$ divise $\psi(2m)$.

Soit $m \geqslant 1$. Pour tout nombre premier p, on note α_p l'entier tel que $p^{\alpha_p} \leqslant 2m < p^{\alpha_p+1}$.

Alors :

$$\psi(2m) = \prod_{p \leqslant 2m} p^{\alpha_p}.$$

Soit p un nombre premier fixé, $p \leqslant 2m$ (car si $p > 2m$, p ne divise ni m ni C_{2m}^m).

Considérons β_p la valuation p-adique de C_{2m}^m et γ_p la valuation p-adique de m.

D'après le lemme 3.7 précédent,

$$\beta_p = \nu_p(C_{2m}^m) = \nu_p\left(\frac{(2m)!}{(m!)^2}\right) = \nu_p((2m)!) - 2\,\nu_p(m!) = \sum_{k=1}^{\alpha_p} \left(\left\lfloor \frac{2m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor \right).$$

Or, si $x \in \mathbb{R}$, on a $x < \lfloor x \rfloor + 1$, d'où :

$$2\lfloor x \rfloor - 1 \leqslant 2x - 1 < \lfloor 2x \rfloor < 2x + 1 < 2\lfloor x \rfloor + 2.$$

D'où $-1 < \underbrace{\lfloor 2x \rfloor - 2\lfloor x \rfloor}_{\in \mathbb{Z}} < 2$. On en déduit $0 \leqslant \lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1$ si bien que chacun des termes présents dans la somme précédente vaut 0 ou 1. Il s'ensuit que $\beta_p \leqslant \alpha_p$.

De plus, la valuation p-adique de $m\,C_{2m}^m$ est $\beta_p + \gamma_p$.

Si $\gamma_p = 0$, on a bien $\beta_p + \gamma_p \leqslant \alpha_p$.

Sinon, pour $1 \leqslant k \leqslant \gamma_p$, l'entier p^i divise m et donc $\left\lfloor \frac{2m}{p^k} \right\rfloor - 2\left\lfloor \frac{m}{p^k} \right\rfloor = 0$. Ainsi, les γ_p premiers termes de la somme sont nuls et les $\alpha_p - \gamma_p$ restants sont au plus égaux à 1, d'où $\beta_p \leqslant \alpha_p - \gamma_p$.

On a donc dans tous les cas $\beta_p + \gamma_p \leqslant \alpha_p$, ce qui assure que la valuation p-adique de $m\,C_{2m}^m$ est *au plus* celle de $\psi(2m)$.

Ce résultat étant valable pour tout p premier, on a : $\psi(2m) \geqslant m\,C_{2m}^m \geqslant 4^m$ d'après le lemme 3.6.

D'où, si l'on considère $n = 2m$, nombre pair supérieur ou égal à 8, $\psi(n) \geqslant 2^n$.

Ainsi, on obtient bien le résultat $\bigvee_{i=1}^n i \geqslant 2^n$ pour tout $n \geqslant 7$. □

3.3.2 Polynômes cyclotomiques

Définition 3.2. *Soit $n \in \mathbb{N}^*$.*

On appelle n-ième ***polynôme cyclotomique***[5]*, ou* ***polynôme de division du cercle en n parties égales****, le produit $\Phi_n = \prod_\zeta (X - \zeta)$ où ζ décrit les racines primitives n-ièmes de l'unité dans $\mathbb{C}$.*

Proposition 3.2. *Φ_n est un polynôme unitaire à coefficients entiers de degré $\varphi(n)$.*

On a la relation :

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Démonstration : Chaque racine n-ième de l'unité dans $\mathbb{C}$ a un unique ordre multiplicatif qui est un diviseur de n d'après la deuxième version du théorème de Lagrange ; autrement dit, il est possible de partitionner les racines n-ièmes de l'unité suivant leur ordre, lesquelles racines sont les zéros de Φ_d pour $d \mid n$. On obtient bien la relation annoncée.

Φ_n est clairement unitaire de degré $\varphi(n)$.

Montrons par récurrence sur n que ses coefficients sont entiers.

On a $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

Par hypothèse de récurrence, les facteurs du produit, sauf justement Φ_n, sont à coefficients entiers. On peut alors écrire dans $\mathbb{C}[X]$: $X^n - 1 = \Phi_n(X) \cdot P(X)$ où P est un polynôme unitaire de $\mathbb{Z}[X]$. Mais par unicité de la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$, on en déduit $\Phi_n \in \mathbb{Z}[X]$. □

Proposition 3.3. *Soient $p, r \in \mathbb{N}$, p premier et $p \wedge r = 1$.*

Le polynôme cyclotomique Φ_r se décompose dans $\mathbb{F}_p[X]$ en un produit de polynômes unitaires irréductibles[6] *de même degré $k = \omega_r(p)$.*

Démonstration : Soit Q un tel facteur de degré s. On note $K = {}^{\mathbb{F}_p[X]}\!/_{Q\mathbb{F}_p[X]}$.

$|K| = p^s$ et tout élément non nul α de K satisfait $\alpha^{p^s-1} = 1$ d'après la troisième version du théorème de Lagrange. Le corps K contient par construction une racine de Φ_r, qui est une racine primitive r-ième de l'unité, disons ζ. Puisque $\zeta^{p^s-1} = 1$, $r \mid p^s - 1$ donc $p^s \equiv 1\ [r]$ et $s \geqslant k$.

Inversement, puisque $\zeta^r = 1$ et que $r \mid p^k - 1$, on a $\zeta^{p^k} = \zeta$. Le sous-corps de K formé des racines de l'équation $X^{p^k} = X$ contient ζ, donc est égal à K tout entier, étant donné que ζ est un élément primitif de K. On a donc $p^s = |K| \leqslant p^k$; d'où $s \leqslant k$.

En définitive, $s = k$, d'où le résultat. □

[5] « Cyclotomie » signifie « division du cercle » en grec : κύκλος, *le cercle*, et τόμος, *la portion*.

[6] Ces polynômes sont en fait tous distincts.

3.4 Démonstration de la validité de l'algorithme

3.4.1 Premier pas

Proposition 3.4. *Si n est premier, l'algorithme retourne que n est* PREMIER.

Démonstration : Si n est premier, alors les étapes 1 et 3 ne peuvent clairement retourner que n est COMPOSÉ. La relation fondamentale démontrée à la proposition 2.1 assure que l'étape 5 ne peut retourner que n est COMPOSÉ. En conséquence, l'algorithme identifie la primarité de n soit à l'étape 4, soit à l'étape 6. □

La réciproque de cette proposition requiert un peu plus de travail. Si l'algorithme identifie la primarité de n à l'étape 4, alors n est bien un nombre premier puisque la troisième étape aurait sinon trouvé un diviseur non trivial de n. Le seul cas restant à étudier est donc celui où l'algorithme retourne que n est PREMIER à la *sixième étape*. Dans la suite de la démonstration, on supposera donc que tel est le cas.

L'algorithme est composé de deux étapes principales — la deuxième et la cinquième : l'étape 2 détermine un nombre r approprié tandis que l'étape 5 vérifie la congruence pour un certain nombre d'entiers a.

3.4.2 Encadrement de r

Lemme 3.8. *Il existe un entier $r \leqslant \lceil 16\log(n)^5 \rceil$ tel que $\omega_r(n) > 4\log(n)^2$.*

Preuve : Soient $r_1, r_2, \ldots, r_t$ tous les nombres tels que $\omega_{r_i}(n) \leqslant 4\log(n)^2$. C'est un ensemble dénombrable puisque si $r > n^{4\log(n)^2}$, $\omega_r(n) > 4\log(n)^2$.

Chacun de ces nombres divise le produit

$$\Delta = \prod_{i=1}^{\lfloor 4\log(n)^2 \rfloor} (n^i - 1)$$

car si $1 \leqslant i \leqslant t$, $n^{\omega_{r_i}(n)} \equiv 1\ [r_i]$, d'où r_i divise $n^{\omega_{r_i}(n)} - 1$ qui apparaît dans le produit puisque $\omega_{r_i}(n) \in [\![1, \lfloor 4\log(n)^2 \rfloor]\!]$.

$$\begin{aligned}
\Delta &= (n-1)(n^2-1)(n^3-1)\cdots(n^{\lfloor 4\log(n)^2\rfloor}-1) \\
&< n\cdot n^2\cdot n^3\cdots n^{\lfloor 4\log(n)^2\rfloor} = n^{1+2+\cdots+\lfloor 4\log(n)^2\rfloor} = n^{\frac{1}{2}\lfloor 4\log(n)^2\rfloor\left(\lfloor 4\log(n)^2\rfloor+1\right)} \\
&< n^{\lfloor 4\log(n)^2\rfloor^2} \\
&< n^{\lfloor 16\log(n)^4\rfloor}
\end{aligned}$$

car si $x \geqslant 1$, $\frac{1}{2}x(x+1) \leqslant x^2 \Leftrightarrow 0 \leqslant x^2 - x$, ce qui est toujours vérifié, d'où la validité de la majoration dès que $n \geqslant 2$ car alors $4\log(n)^2 \geqslant 4$.

Donc $\Delta < 2^{\lfloor 16\log(n)^5 \rfloor}$ car $n = 2^{\log_2(n)}$.

D'après la proposition 3.1, le plus petit commun multiple des $\lceil 16\log(n)^5 \rceil$ premiers nombres est au moins $2^{\lceil 16\log(n)^5 \rceil}$. Si tous les nombres r inférieurs ou égaux à $\lceil 16\log(n)^5 \rceil$ vérifiaient $\omega_r(n) \leqslant 4\log(n)^2$, ils diviseraient tous Δ et $\bigvee_{i=1}^{\lceil 16\log(n)^5 \rceil} i \leqslant \Delta$, ce qui est exclu d'après la majoration ci-dessus.

En conséquence, il existe un entier $r \leqslant \lceil 16\log(n)^5 \rceil$ tel que $\omega_r(n) > 4\log(n)^2$. □

3.4.3 Application de l'introspection

Soit p un diviseur premier de n.

On a $p > r$ car sinon la troisième ou la quatrième étape aurait conduit à l'obtention de la non-primarité ou de la primarité de n. Du moment que n et r sont premiers entre eux (sinon ces deux mêmes étapes auraient correctement identifié n), p et n sont inversibles dans $\mathbb{Z}/r\mathbb{Z}$.

Les nombres p et r sont dorénavant fixés dans la suite de la démonstration.

Notons aussi $l = \lfloor 2\sqrt{\varphi(r)}\,\log(n) \rfloor$.

La cinquième étape de l'algorithme vérifie l équations. Puisque l'algorithme ne retourne pas que n est Composé lors de cette étape, on a :

$$(X+a)^n \equiv X^n + a \quad [X^r - 1,\ n] \quad \text{pour tout } 1 \leqslant a \leqslant l.$$

D'où :

$$(X+a)^n \equiv X^n + a \quad [X^r - 1,\ p] \quad \text{pour tout } 1 \leqslant a \leqslant l$$

car $p \mid n$ et en vertu de l'identité remarquable, on a, comme p est premier :

$$(X+a)^p \equiv X^p + a \quad [X^r - 1,\ p] \quad \text{pour tout } 1 \leqslant a \leqslant l.$$

Donc n se comporte comme le nombre premier p dans l'équation ci-dessus. D'après les résultats liminaires sur l'introspection (partie 3.2.3), il est clair que n et p sont introspectifs pour $X + a$ ($1 \leqslant a \leqslant l$) et donc que tout nombre dans l'ensemble $\mathcal{I} = \{n^i \cdot p^j \mid i, j \geqslant 0\}$ est introspectif pour tout polynôme dans l'ensemble $\mathcal{P} = \{\prod_{i=1}^{l} (X+a)^{\lambda_i} \mid \lambda_i \geqslant 0\}$.

Définissons maintenant à partir de ces ensembles deux groupes qui vont jouer un rôle crucial dans la suite de la démonstration.

Le premier groupe $\mathcal{G}$ est l'ensemble des résidus des nombres de $\mathcal{I}$ modulo r. C'est un sous-groupe de $(\mathbb{Z}/r\mathbb{Z})^\star$ puisque $n \wedge r = p \wedge r = 1$ comme nous l'avons déjà observé ; donc n et r y sont inversibles.

Notons $t = |\mathcal{G}|$ le cardinal de $\mathcal{G}$. Le groupe $\mathcal{G}$ est engendré par n et par p modulo r et comme $\omega_r(n) > 4\log(n)^2$, on a $t > 4\log(n)^2$ — il suffit de fixer $j = 0$ et de faire varier i dans la définition de $\mathcal{I}$ pour le constater.

Pour définir le second groupe, considérons Φ_r le r-ième polynôme cyclotomique sur $\mathbb{F}_p[X]$. D'après les résultats préliminaires sur la cyclotomie (partie 3.3.2), Φ_r divise $X^r - 1$ et se factorise en facteurs irréductibles de degré $\omega_r(p)$. Soit Q un tel facteur irréductible.

Le second groupe $\mathcal{H}$ est l'ensemble des résidus non nuls des polynômes de $\mathcal{P}$ dans $\mathcal{F} = \frac{\mathbb{F}_p[X]}{Q\mathbb{F}_p[X]}$. Ce groupe est engendré par $\{X + a\}_{1 \leqslant a \leqslant l}$ dans le corps $\mathcal{F}$.

$\mathcal{H}$ est un sous-groupe du groupe multiplicatif de $\mathcal{F}$.

3.4.4 Encadrement du cardinal de $\mathcal{H}$

Le cardinal du groupe $\mathcal{H}$ est exponentiel en t :

Lemme 3.9.

$$|\mathcal{H}| \geqslant C_{t+l-2}^{t-1}.$$

Preuve : Notons tout d'abord que les racines de Q sont des racines primitives r-ièmes de l'unité dans $\mathcal{F}$ puisque Q est un facteur du polynôme cyclotomique Φ_r.

Montrons alors qu'à deux polynômes distincts de degré strictement inférieur à t dans $\mathcal{P}$ correspondent deux résidus différents dans $\mathcal{H}$. Considérons deux tels polynômes distincts A et B dans $\mathcal{P}$ et supposons par l'absurde que $A \equiv B$ dans $\mathcal{F}$.

Soit $m \in \mathcal{I}$. Nous avons aussi $A(X)^m \equiv B(X)^m$ dans $\mathcal{F}$. Puisque m est introspectif à la fois pour A et pour B et que Q divise $X^r - 1$, on obtient : $A(X^m) \equiv B(X^m)$ dans $\mathcal{F}$. Cela implique que ζ^m est une racine du polynôme $R(Y) = A(Y) - B(Y)$ pour tout $m \in \mathcal{G}$.

Comme $m \wedge r = 1$ — $\mathcal{G}$ est un sous-groupe de $(\mathbb{Z}/r\mathbb{Z})^\star$ —, chaque ζ^m est une racine primitive r-ième de l'unité. R a alors $t = |\mathcal{G}|$ racines distinctes dans $\mathcal{F}$.

Les racines ζ^m sont distinctes et

$$\prod_{\substack{m \in \mathcal{G} \\ m \wedge r = 1}} (X - \zeta^m) = \Phi_r \text{ divise } R \text{ dans } \mathcal{F} \text{ et donc dans } \mathbb{F}_p[X].$$

D'où $A \equiv B$ dans $\frac{\mathbb{F}_p[X]}{\Phi_r \mathbb{F}_p[X]}$. Or $\deg(\Phi_r) = \varphi(r) \geqslant t$ puisque les éléments inversibles de $\mathbb{Z}/r\mathbb{Z}$ sont au nombre de $\varphi(r)$; donc $A \equiv B$ dans $\mathbb{F}_p[X]$, ce qui est contradictoire avec A et B distincts dans $\mathcal{P}$.

On a ainsi démontré $A \not\equiv B$ dans $\mathcal{F}$.

Remarquons en outre que $i \neq j$ dans $\mathbb{F}_p$ pour $1 \leqslant i \neq j \leqslant l$ puisque $l < r < p$. En effet, $l = \lfloor 2\sqrt{\varphi(r)}\,\log(n) \rfloor < 2\sqrt{r}\log(n) < r$ car $4\log(n)^2 \leqslant \omega_r(n) < r$ conformément au théorème d'Euler 3.1. Donc les polynômes $\{X + a\}_{1 \leqslant a \leqslant l}$ sont tous distincts dans $\mathcal{F}$.

Si $X + a = 0$ dans $\mathcal{F}$ pour un $a \leqslant l$ — ce qui se produit lorsque $Q = X + a$ —, $X + a$ n'est alors pas inclus dans le groupe $\mathcal{H}$ puisque son résidu y est nul ; il existe donc au moins $l - 1$ polynômes distincts du *premier degré* dans $\mathcal{H}$. Il existe en conséquence au moins C_{t+l-2}^{t-1} polynômes distincts de degré strictement inférieur à t dans $\mathcal{H}$ d'après le résultat établi au lemme 3.3.

Il s'ensuit alors que $|\mathcal{H}| \geqslant C_{t+l-2}^{t-1}$. □

Dans l'hypothèse où n n'est pas une puissance de p, le cardinal de $\mathcal{H}$ est aussi majoré exponentiellement en t :

Lemme 3.10. *Si n n'est pas une puissance de p, alors :*

$$|\mathcal{H}| < \frac{1}{2}\, n^{2\sqrt{t}}.$$

Preuve : Considérons le sous-ensemble $\mathcal{J}$ de $\mathcal{I}$ défini par :

$$\mathcal{J} = \left\{ n^i \cdot p^j \mid 0 \leqslant i, j \leqslant \lfloor \sqrt{t} \rfloor \right\}.$$

Si n n'est pas une puissance de p, alors l'ensemble $\mathcal{J}$ comporte $(\sqrt{t} + 1)^2 > t$ nombres distincts. Puisque $t = |\mathcal{G}|$, au moins deux des nombres de $\mathcal{J}$ sont égaux modulo r en vertu du principe des tiroirs de Dirichlet-Schläfli. Si l'on note $m_1 > m_2$ ces deux nombres, il vient :

$$X^{m_1} \equiv X^{m_2} \quad [X^r - 1,\ p].$$

Soit $P \in \mathcal{P}$. Alors :

$$P(X)^{m_1} \equiv P(X^{m_1}) \equiv P(X^{m_2}) \equiv P(X)^{m_2} \quad [X^r - 1,\ p].$$

Il s'ensuit que $P(X)^{m_1} \equiv P(X)^{m_2}$ dans le corps $\mathcal{F}$. Subséquemment, $P(X) \in \mathcal{H}$ est une racine du polynôme $R(Y) = Y^{m_1} - Y^{m_2}$ dans $\mathcal{F}$; et comme $P(X)$ est un élément arbitraire de $\mathcal{H}$, le polynôme $R(Y)$ possède au moins $|\mathcal{H}|$ racines distinctes dans $\mathcal{F}$.

Or le degré de $R(Y)$ est

$$m_1 \leqslant \max(\mathcal{J}) = (n \cdot p)^{\lfloor \sqrt{t} \rfloor} < \frac{1}{2}\, n^{2\sqrt{t}}$$

car p divise n avec $p \neq n$ par hypothèse du lemme, d'où $p < \frac{1}{2}\, n$. Cela montre que $|\mathcal{H}| < \frac{1}{2}\, n^{2\sqrt{t}}$. □

3.4.5 Théorème fondamental

Avec ces estimations de la taille de $\mathcal{H}$, nous pouvons enfin prouver la validité de l'algorithme :

Théorème 3.2. *L'algorithme retourne que n est* PREMIER *si, et seulement si, n est premier.*

Démonstration : On a déjà vu à la proposition 3.4 que si n est premier, l'algorithme indique que n est PREMIER.

Réciproquement, supposons que l'algorithme retourne que n est PREMIER.
D'après le lemme 3.10 précédent, pour $t = |\mathcal{G}|$ et $l = \lfloor 2\sqrt{\varphi(r)}\,\log(n) \rfloor$, on a :

$$
\begin{aligned}
|\mathcal{H}| &\geqslant C_{t+l-2}^{t-1} \\
&\geqslant C_{l-1+\lfloor 2\sqrt{t}\,\log(n)\rfloor}^{\lfloor 2\sqrt{t}\,\log(n)\rfloor} && \text{car } t > 2\sqrt{t}\,\log(n) \text{ puisque } t > 4\log(n)^2. \\
&\geqslant C_{2\lfloor 2\sqrt{t}\,\log(n)\rfloor - 1}^{\lfloor 2\sqrt{t}\,\log(n)\rfloor} && \text{car } l = \left\lfloor 2\sqrt{\varphi(r)}\,\log(n) \right\rfloor \geqslant \left\lfloor 2\sqrt{t}\,\log(n) \right\rfloor. \\
&\geqslant 2^{\lfloor 2\sqrt{t}\,\log(n)\rfloor} && \text{car } 2\sqrt{t}\,\log(n) \geqslant 3 \text{ par le lemme 3.1.} \\
&\geqslant 2^{\log\left(n^{2\sqrt{t}}\right)} \\
&\geqslant n^{2\sqrt{t}} \\
|\mathcal{H}| &\geqslant \frac{1}{2}\, n^{2\sqrt{t}}.
\end{aligned}
$$

Or, d'après le lemme 3.9, $|\mathcal{H}| < \frac{1}{2}\, n^{2\sqrt{t}}$ lorsque n n'est pas une puissance de p. Il s'ensuit qu'il existe $k > 0$ tel que $n = p^k$.

Mais si $k > 1$, l'algorithme aurait alors retourné que n est COMPOSÉ lors de la première étape. Par conséquent $k = 1$ et $n = p$.

Donc n est premier. □

Ceci achève la démonstration de la validité de l'algorithme. Il ne reste plus qu'à vérifier que l'algorithme $\mathcal{AKS}$ s'exécute effectivement en temps polynomial.

4 Complexité de l'algorithme

4.1 Complexité dans sa forme actuelle

On utilisera la notation $\Omega(t(n))$ pour $O(t(n) \cdot P(\log(t(n))))$ où P est une fonction polynomiale. Par exemple, $\Omega(\log(n)^k) = O(\log(n)^k \cdot P(\log(\log(n)))) = O(\log(n)^{k+\varepsilon})$ pour tout $\varepsilon > 0$, qui est donc aussi un temps polynomial.

On considérera dans les calculs de complexité temporelle que l'addition, la multiplication et la division de deux nombres de m bits peuvent être réalisées en un temps $\Omega(m)$.

Théorème 4.1. *La complexité asymptotique temporelle de l'algorithme est $\Omega(\log(n)^{10.5})$.*

Démonstration : La première étape de l'algorithme requiert un temps asymptotique en $\Omega(\log(n)^3)$.

Durant la deuxième étape, on cherche un naturel r tel que $\omega_r(n) > 4\log(n)^2$. On peut y parvenir en essayant successivement les valeurs de r et en regardant si $n^k \not\equiv 1\ [r]$ pour tout $k \leqslant 4\log(n)^2$. Pour

un r fixé, cela demande $O(\log(n)^2)$ multiplications modulo r, d'où un temps en $\Omega(\log(n)^2 \log(r))$. Or le lemme 3.8 indique que seuls $O(\log(n)^5)$ différents r ont besoin au maximum d'être testés, ce qui donne une complexité en $\Omega(\log(n)^7)$.

La troisième étape consiste en le calcul du plus grand commun diviseur de r nombres. Chacun de ces calculs, réalisés à l'aide de l'algorithme d'Euclide, requiert[7] un temps en $O(\log(n))$, donc la complexité est $O(r \log(n)) = O(\log(n)^6)$.

La quatrième étape s'exécute en seulement $O(\log(n))$ puisque c'est une comparaison dont la complexité ne dépend que de la longueur de n.

Lors de la cinquième étape, $\lfloor 2\sqrt{\varphi(r)}\ \log(n) \rfloor$ congruences sont testées.
Chacune requiert $O(\log(n))$ multiplications de polynômes de degré r dont les coefficients sont de taille $O(\log(n))$, donc peut être vérifiée en $\Omega(r \log(n)^2)$. Aussi la complexité de cette étape est-elle en :
$\Omega(r\sqrt{\varphi(r)}\ \log(n)^3) = \Omega(r^{\frac{3}{2}} \log(n)^3) = \Omega(\log(n)^{10.5})$.

Ce temps domine tous les autres : c'est donc la complexité cherchée de l'algorithme. □

Il n'en faut pas moins noter que la complexité temporelle de l'algorithme peut être améliorée en trouvant un majorant plus fin de r, ce qui est établi dans le lemme 3.8. Bien entendu, le meilleur scénario serait pour r de l'ordre de $O(\log(n)^2)$ puisque la complexité de l'algorithme serait alors en $\Omega(\log(n)^6)$.
En fait, deux conjectures laissent penser qu'un tel naturel r existe, ce qui est d'ailleurs vérifié heuristiquement dans la pratique.

4.2 Complexité dans une forme améliorée

4.2.1 Conjecture d'Artin

Conjecture 4.1. *Soient $m, n \in \mathbb{N}$ avec n non carré parfait. Alors le nombre de nombres premiers $q \leqslant m$ pour lesquels $\omega_q(n) = q - 1$ est asymptotiquement $\frac{A\,m}{\ln(m)}$ où A désigne la constante d'Artin :*

$$A = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^2 - p}\right) \approx 0.37.$$

Si la conjoncture d'Artin est vraie pour m de l'ordre de $O(\log(n)^2)$, on a immédiatement l'existence de r de l'ordre de $O(\log(n)^2)$ répondant aux propriétés recherchées. Avec un tel r, l'algorithme a une complexité en $O(\log(n)^6)$.

Notons que cette conjecture fut néanmoins démontrée par Hooley en 1967 à l'aide de l'hypothèse de Riemann généralisée (1859) relative aux fonctions ζ, à savoir que lorsque la partie réelle de $s \in \mathbb{C}$ est strictement comprise entre 0 et 1, les zéros de

$$\zeta(s) = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)$$

ont tous $1/2$ pour partie réelle.

Non prouvée aujourd'hui, cette hypothèse est considérée comme l'un des problèmes majeurs actuels ; elle est étroitement liée à la distribution des nombres premiers prouvée par Hadamard et

[7] Gabriel Lamé montra en effet ce résultat en 1845 par le truchement de la suite de Fibonacci. Édouard Lucas prouva ensuite que cela constitue le résultat optimal.

de La Vallée-Poussin en 1896, $\pi(n) \underset{+\infty}{\sim} \dfrac{n}{\ln(n)}$, et fit l'objet du huitième problème de Hilbert énoncé en 1900. Sa résolution a d'ailleurs été mise à prix en mai 2000 par le *Clay Mathematics Institute* pour un million de dollars.

Quelques avancées ont néanmoins été faites, notamment par André Weil. Gram prouva en 1903 que les quinze premiers zéros sont bien d'abscisse $\frac{1}{2}$ puis Hardy prouva l'existence d'une infinité de tels zéros en 1914. Ceux-ci sont denses sur l'axe critique. Des zones d'exclusion des zéros non triviaux ont par la suite été trouvées et l'on a pu calculer numériquement des millions de zéros, sans jamais trouver de contre-exemples. C'est pourquoi la communauté mathématique tend à considérer la conjecture de Riemann comme *vraie*.

4.2.2 Conjecture de la densité des nombres premiers de Sophie Germain

Conjecture 4.2. *Soient $m, n \geqslant 2$.*
Le nombre de nombres premiers $m \leqslant n$ tels que $2m+1$ soit aussi premier est asymptotiquement

$$\frac{2\,C_2\,n}{\ln(n)^2} \quad \text{où} \quad C_2 = \prod_{p>2 \text{ premier}} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0,66$$

est la constante des nombres premiers jumeaux.
De tels nombres m sont dit nombres premiers de Sophie Germain.

Si cette conjecture est vraie, on en déduit que r est de l'ordre de $\Omega(\log(n)^2)$. Avec un tel r, l'algorithme possède alors une complexité en $\Omega(\log(n)^6)$.

Notons que des progrès ont aussi été réalisés dans l'établissement de cette conjecture.

Une étude empirique permet d'ailleurs de trouver que l'algorithme possède une complexité de l'ordre de $1000\log(n)^6$, ce qui est en accord parfait avec les deux conjectures précédentes.

4.2.3 Amélioration de l'identité remarquable

Dans l'algorithme, la boucle exécutée lors de la cinquième étape doit être réalisée au plus $\lfloor 2\sqrt{\varphi(r)}\,\log(n)\rfloor$ fois afin de s'assurer que le cardinal du groupe $\mathcal{H}$ est dépassé.

Le nombre d'itérations de la boucle peut être réduit si l'on montre qu'il existe un système générateur de $\mathcal{H}$ plus petit que $\{X+a\}_{1\leqslant a\leqslant l}$, ce qui semble très vraisemblable.

On peut alors même améliorer la complexité de l'algorithme jusqu'à $\Omega(\log(n)^3)$ si la conjecture suivante s'avère vraie :

Conjecture 4.3. *Soient $n, r \in \mathbb{N}$ tels que :*
- *r est un nombre premier qui ne divise pas n*
- *$(X-1)^n \equiv X^n - 1 \quad [X^r - 1,\ n]$*

Dans ces conditions,

$$n \text{ est premier ou } n^2 \equiv 1 \quad [r].$$

Cette conjecture fut vérifiée pour $r \leqslant 100$ et $n \leqslant 10^{10}$ par Kayal et Saxena. Si elle est vraie, l'algorithme pourrait alors être modifié de sorte à d'abord chercher un entier r qui ne divise pas n^2-1 ; un tel r peut alors être trouvé dans l'intervalle $[\![2, 4\log(n)]\!]$, en utilisant le lemme que le produit de tous les nombres premiers inférieurs à n est asymptotiquement supérieur à e^n. Ensuite, la congruence de la cinquième étape est à vérifier pour l'entier r ainsi déterminé, ce qui requiert un temps en $\Omega(r\log(n)^2)$.

Avec ce test différent pour la cinquième étape, l'algorithme aurait alors une complexité en $\Omega(\log(n)^3)$, ce qui le rendrait très compétitif et utilisable en pratique.

5 Implémentation de l'algorithme

5.1 Version en $\mathcal{M}$APLE

Il est possible d'implémenter l'algorithme *à vue* dans un langage de calcul formel. Toutefois, on remarque aussitôt que le temps de calcul devient rapidement rédhibitoire, quand bien même les nombres testés sont relativement petits. Assurément, si l'on utilise la fonction prédéfinie *isprime* de $\mathcal{M}$APLE, le même résultat est donné en moins d'un dixième de seconde pour de tels nombres, et en quelques dizaines de secondes pour des nombres de plus de six cents chiffres.

Toutefois, la documentation de $\mathcal{M}$APLE précise que la fonction *isprime* est un test probabiliste de non-primarité, en ce sens qu'il subsiste toujours une probabilité d'erreur lorsque cette fonction retourne que n est PREMIER.

Nonobstant, *« aucun contre-exemple n'est connu et il est conjecturé qu'un tel exemple comporte plusieurs centaines de chiffres »*.

Il n'en reste pas moins que le test *isprime* n'est pas déterministe, au contraire de l'algorithme $\mathcal{AKS}$.

5.2 Limites d'une telle implémentation

Notons que la fonction inerte *Powmod* de $\mathcal{M}$APLE, qui permet de calculer des puissances de polynômes, voit ses capacités dépassées pour de grandes valeurs de r et de n.

Il est aussi assuré que la complexité de l'algorithme n'est pas optimale : il faudrait en fait implémenter des outils complexes de calculs rapides, de multiplication de polynômes à base de transformée de FOURIER rapide et de congruences modulo un polynôme, pour ne citer que ces exemples.

En outre, ce n'est pas un langage de calcul symbolique comme $\mathcal{M}$APLE qui convient pour ce genre d'algorithme ; un langage de programmation plus avancé et optimisé, tel le C++ ou le C#, donnerait des résultats beaucoup plus satisfaisants. Mais une telle implémentation requerrait beaucoup plus de travail.

5.3 Autres implémentations de l'algorithme

De nombreuses personnes ont proposé une implémentation de l'algorithme $\mathcal{AKS}$ en divers langages de programmation.

En pratique, les tests de MILLER sont beaucoup plus rapides, bien qu'ils soient quand même lents à cause du calcul de nombreuses exponentielles modulaires ; l'algorithme à base de courbes elliptiques dû à ATKIN est à même de prouver la primarité de nombres de 512 bits en une seconde, de 1024 bits en une minute, et des nombres de l'ordre de $2^{10\,000}$ en un temps « raisonnable » (un mois) sur un Pentium-III à 450 MHz. Ce dernier algorithme, *supposé* polynomial, est néanmoins probabiliste ; un avantage est qu'il fournit en outre un certificat vérifiable polynomialement en $O(\log(n)^4)$.

Il n'en faut pas moins oublier que, quoique la complexité temporelle de l'algorithme soit polynomiale, sa complexité spatiale n'est pas du tout optimisée. L'algorithme nécessite en effet beaucoup de mémoire lors de son utilisation et conduit à la manipulation de données volumineuses.

De plus, l'entier r qui est déterminé par l'algorithme $\mathcal{AKS}$ n'est pas le plus petit qui puisse convenir pour les tests de la cinquième étape. Pour $n = 2^{512}$, l'entier r le plus optimiste est de l'ordre de $16 \cdot 10^6$, ce qui conduit à manipuler des polynômes denses de plus de 1 gigaoctet comportant plusieurs dizaines de milliers de termes, ce qui est peut-être envisageable.

Le test de la primarité du nombre $n = 10^9 + 7$ prend une semaine sur un PC à 700 MHz avec l'algorithme normal, en utilisant $\mathcal{GMP}$ 4.1 : chaque calcul intermédiaire dure 44 secondes à cause du degré élevé des polynômes manipulés. En fait, il est possible de trouver un entier r plus petit

($r = 359$ au lieu de 57 287) qui conduit à un temps de *6 minutes et 9 secondes*, ce qui constitue un net progrès et rend l'algorithme utilisable en pratique.

Pour l'anecdote, on estime que 10^{25} opérations élémentaires ont été réalisées par l'ensemble des microprocesseurs d'ordinateur depuis qu'ils existent. En ne tenant pas compte des problèmes de mémoire spatiale, c'est le nombre d'opérations nécessaires à l'algorithme $\mathcal{AKS}$ pour déterminer la primarité d'un nombre à 100 000 chiffres. Or, sachant que les plus grands nombres premiers connus ont plus de quatre millions de chiffres, on se rend bien compte de l'inefficacité pratique de cet algorithme...

6 Conclusion

6.1 Applications de l'algorithme $\mathcal{AKS}$

À l'heure actuelle, il n'existe aucune application réalisable de l'algorithme, indique Agrawal lui-même : ce dernier préfère considérer le problème comme un *« défi intellectuel »*.

Interrogé sur le dépôt d'un éventuel brevet sur l'algorithme, Agrawal se montre d'ailleurs catégoriquement opposé, bien que l'*Institut Indien de Technologie* eût voulu la protection de l'algorithme.

On peut en conséquence raisonnablement penser que l'algorithme sera efficacement amélioré dans les prochaines années par les mathématiciens. Il suffit en effet de constater la grande différence qui existe entre les deux versions de l'algorithme $\mathcal{AKS}$: en août 2002, sa complexité temporelle est en $\Omega(\log(n)^{12})$ et la démonstration requiert de puissants outils d'analyse et d'algèbre, tandis qu'en mars 2003, elle est en $\Omega(\log(n)^{10.5})$ et la démonstration devient somme toute assez élémentaire dans les moyens usités.

De nombreux mathématiciens et théoriciens se sont en effet penchés sur le problème et ont contribué à l'amélioration de l'algorithme dont de nombreuses variantes ont été trouvées. Dan Bernstein s'est par exemple inspiré de l'idée de l'algorithme pour en réaliser un en $\Omega(\log(n)^4)$, mais non déterministe ; il annonce ainsi la résolution d'un nombre de 300 chiffres en un jour avec une implémentation utilisant la librairie $\mathcal{GMP}$ pour manipuler des grands nombres sur un Pentium-III de 800 MHz.

L'informatique fera aussi des progrès et les ordinateurs seront à même d'exécuter plus rapidement l'algorithme : une différence en rapidité qui va du simple au quintuple est notable pour seulement 300 MHz supplémentaires.

Il est même possible que l'algorithme excelle sur les tests de primarité qui sont actuellement utilisés, notamment dans le domaine de la cryptographie, lorsque de très grands nombres premiers sont nécessaires et qu'aucune erreur ne peut être tolérée sur leur primarité.

6.2 $\mathscr{P} \in \mathcal{P}$

Il résulte ainsi que l'algorithme $\mathcal{AKS}$ se révèle trop lent pour le moment en l'état ; mais nul doute qu'une variante lui permettra de rivaliser avec les algorithmes actuels, à moins que l'une des conjectures énoncées dans la partie 4.2 ne soit démontrée, ce qui conduirait à une complexité temporelle en $\Omega(\log(n)^3)$ dans le meilleur des cas.

Certes l'algorithme demeure de nos jours inutilisable *en pratique* à grande échelle ; cela n'assombrit cependant en rien la beauté du résultat *théorique* établi par les auteurs de l'algorithme, à savoir $\mathscr{P} \in \mathcal{P}$, et qui suscite l'émerveillement de toute la communauté mathématique.

À la lueur de la démonstration de cet algorithme, on peut par ailleurs légitimement se demander si d'autres résultats mathématiques dont la démonstration nous échappe encore, ne posséderaient pas une preuve aussi *« brillante, élégante et simple »* que celle-ci.

Références bibliographiques

[1] Michel DEMAZURE, *Cours d'Algèbre*. Cassini, Nouvelle Bibliothèque Mathématique, 1997.

[2] Neeraj KAYAL et Nitin SAXENA, *Towards a deterministic polynomial-time test.* http://www.cse.iitk.ac.in/research/btp2002/primality.html, avril 2002.

[3] Manindra AGRAWAL, Neeraj KAYAL et Nitin SAXENA, PRIMES *is in* $\mathcal{P}$. http://www.cse.iitk.ac.in/users/manindra/primality_original.pdf, 6 août 2002. http://www.cse.iitk.ac.in/users/manindra/primality.pdf, 4 mars 2003.

[4] François MORAIN, *Primalité théorique et primalité pratique*, 4 octobre 2002.

[5] Folkmar BORNEMANN, PRIMES *is in* $\mathcal{P}$ *: une avancée accessible à « l'homme ordinaire »*. Traduction par Colette ANNÉ dans la *Gazette des Mathématiciens* (n°98, octobre 2003) d'un article paru dans les *Notices de l'*$\mathcal{AMS}$ en mai 2003.

Remarques

La première version de l'algorithme $\mathcal{AKS}$ diffère seulement à l'étape 2 où r est alors un nombre *premier* tel que le plus grand diviseur q de $r-1$ vérifie $q \geqslant 4\sqrt{r}\log(n)$ et $n^{\frac{r-1}{q}} \not\equiv 1\ [r]$.
La complexité de l'algorithme était alors en $O(\log(n)^{12})$.

Relativement aux citations qui agrémentent la première page de l'exposé, Shafi GOLDWASSER, éminent professeur, spécialisée dans le domaine de la cryptographie à l'*Institut de Technologie* de Massachusetts, s'émerveilla ainsi : *« It's the best result I've heard in over ten years ».*

Quant à l'un des meilleurs spécialistes en théorie des nombres, Carl POMERANCE, travaillant pour les laboratoires *Bell*, à peine eut-il discuté durant le déjeuner avec ses collègues sur le nouvel algorithme qu'il organisa précipitamment un séminaire l'après-midi même sur le sujet ; le fait qu'il puisse réaliser si rapidement un tel symposium constitue *« a measure of how wonderfully elegant this algorithm is »*, précisa-t-il : *« This algorithm is beautiful ».*

La citation extraite des *Disquisitiones Arithmeticæ — Recherches Arithmétiques* en français — de GAUSS est, dans le texte latin :

« Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resoluendi, ad grauissima ac utilissima totius Arithmeticæ pertinere, et geometrarum tum ueterum tum recentiorum industriam ac sagacitatem occupauisse, tam notum est, ut de hac re copiose loqui superfluum foret. [...]

« Prætereaque scientiæ dignitas requirere uidetur, ut omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur. »