Le test de primalité polynomial AKS

Joachim STUDNIA

2019

Résumé

Jusqu'au début du XXIe siècle, le problème de l'existence d'un test de primalité polynomial était ouvert. Depuis l'Antiquité, on sait évidemment tester la primalité d'un entier n en $O(\sqrt{n})$, en examinant la divisibilité par tous les entiers inférieurs à $\sqrt{n}$. Cependant, cet algorithme naïf a une complexité exponentielle en la taille de l'entrée (c'est-à-dire $\log_2 n$ bits). Dans ce TIPE, j'étudie l'algorithme AKS (nommé en l'honneur des chercheurs Manindra Agrawal, Neeraj Kayal, et Nitin Saxena) publié en août 2002, qui détermine justement si un entier n donné en entré est premier, en $O^{\sim}(\log^{21/2} n)$.
J'ai tout de suite été fasciné par la preuve de la correction de l'algorithme, à la fois par par la simplicité des outils mis en œuvre, et la variété des arguments. Le sujet choisi relève de la théorie des nombres, mais nombreuses sont les justifications tirées de la théorie des extensions de corps, et des corps finis.
Le but est de comprendre l'ensemble des arguments permettant de justifier la complexité polynomiale de l'algorithme AKS.
Enfin, l'étape ultime du TIPE consiste en l'implémentation du test de primalité sur Python, et d'en déduire si d'éventuelles applications pratiques sont à ce jour envisageables.

1 Notations et rappels

— Si $n \geqslant 1$ et p est premier, on note $\nu_p(n)$ la valuation p-adique de n.

— Si $n \in \mathbb{N}^*$, $(U(\mathbb{Z}/n\mathbb{Z}), \times)$ est le groupe des inversibles de l'anneau commutatif $\mathbb{Z}/n\mathbb{Z}$, d'ordre $\varphi(n)$.

— La notation log désignera dans la suite le logarithme en base 2.

— Si $(G, \cdot)$ est un groupe et $a \in G$, $< a >$ désigne le sous-groupe de G engendré par a.

— La notation $O^{\sim}(t(n))$ désigne une complexité en $O(t(n) \log t(n))$.

— Si $n \geqslant 1$ et a est premier avec n, alors on note $\mathrm{ord}_n(a)$ l'ordre de $\bar{a}$ dans $(U(\mathbb{Z}/n\mathbb{Z}), \times)$

— Si K est un corps (commutatif), et $P \in K[X] \setminus \{0\}$, on note (P) l'idéal de $K[X]$ engendré par P, et $K[X]/(P)$ l'algèbre quotient de $K[X]$ par cet idéal, qui est un K-espace vectoriel de dimension $\deg P$. De plus,

$$P \text{ irréductible dans } K[X] \iff K[X]/(P) \text{ est un corps}$$

Enfin, si $K = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ avec p premier, et $P \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductible de degré d, alors $(\mathbb{Z}/p\mathbb{Z}[X])/(P)$ devient un corps qui est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension d, donc de cardinal p^d.

— Si K est un corps, on note $\mathrm{car}\, K \in \mathbb{N}$ sa caractéristique, qui est soit nulle, soit un nombre premier.

— Si $K \subset L$ sont deux corps, alors on note $[L : K]$ la dimension de L vu comme K-espace vectoriel.

2 Introduction

Lemme 2.1. Soit $n \geqslant 2$ et $a \in \mathbb{Z}$ avec $\mathrm{pgcd}(a, n) = 1$. Alors

$$n \text{ est premier } \iff (X + a)^n = X^n + a \text{ dans } \mathbb{Z}/n\mathbb{Z}[X] \tag{1}$$

Remarque. Notons tout de suite que l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est *a priori* pas intègre, donc l'anneau $\mathbb{Z}/n\mathbb{Z}[X]$ non plus.

Preuve.
$\Longrightarrow$ Si $n = p$ est premier, alors pour $k \in [\![1, p-1]\!]$, on sait que $p|\binom{p}{k}$. De plus, comme $a^p \equiv a \pmod p$, on a bien $(X+a)^p = X^p + a$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ après développement.
$\Longleftarrow$ Par contraposée. Si n n'est pas premier, fixons $p \in [\![1, n-1]\!]$ un diviseur premier de n, et soit $c = \nu_p(n) \geqslant 1$. Alors $\nu_p(n(n-1)\dots(n-(p-1))) = c$, donc $\nu_p(\binom{n}{p}) = c-1$. Ainsi, comme $p \nmid a$, on a $p^c \nmid \binom{n}{p} a^{n-p}$, donc $\binom{n}{p} a^{n-p} \not\equiv 0 \pmod n$. Ainsi, $(X+a)^n \neq X^n + a$ dans $\mathbb{Z}/n\mathbb{Z}[X]$. □

Dès lors, un test de primalité envisageable serait de prendre un entier n, un entier a premier avec n, et de regarder si $(X+a)^n = X^n + a$ dans $\mathbb{Z}/n\mathbb{Z}[X]$. Cependant, ceci prendrait un temps $O(n)$ exponentiel que l'on veut précisément éviter. Dans la suite, l'idée sera de choisir un entier $r \geqslant 1$, et de regarder si l'égalité (1) a lieu dans $(\mathbb{Z}/n\mathbb{Z}[X])/(X^r - 1)$, *ie* si

$$\overline{(X+a)^n} = \overline{X^n + a} \text{ dans } (\mathbb{Z}/n\mathbb{Z}[X])/(X^r-1) \tag{2}$$

Ainsi, si n est premier, alors (2) est vraie pour tout a premier avec n d'après le lemme. Mais il est possible que n soit composé et que (2) soit encore vraie pour un certain couple (a, r). On verra cependant que si (2) est vraie pour un r bien choisi, et suffisamment de a, alors n est nécessairement une puissance d'un nombre premier. Comme le nombre de a à tester et le r convenable seront bornés par des polynômes en $\log n$, on aura un algorithme déterministe polynomial de test de primalité (moyennant un algorithme polynomial pour tester si un entier est une puissance parfaite).

Lemme 2.2. Soit $n \geqslant 7$. Alors $\operatorname{ppcm}_{1 \leqslant i \leqslant n} i \geqslant 2^n$.

Preuve. Voir annexe. □

3 Description et correction de l'algorithme

Algorithme.
Entrée : $n \geqslant 2$ entier

1. Si ($n = a^b$ où $b \geqslant 2$), renvoyer COMPOSÉ
2. Trouver le plus petit r premier avec n tel que $\mathrm{ord}_r(n) > \log^2 n$
3. Si $1 < \mathrm{pgcd}(a, n) < n$ pour un certain $1 \leqslant a \leqslant r$, renvoyer COMPOSÉ
4. Si $n \leqslant r$, renvoyer PREMIER
5. Pour a allant de 1 à $\lfloor \sqrt{\varphi(r)} \log n \rfloor$,
   si $\overline{(X+a)^n} \neq \overline{X^n + a}$ dans $(\mathbb{Z}/n\mathbb{Z}[X])/(X^r-1)$, renvoyer COMPOSÉ
6. Renvoyer PREMIER

Lemme 3.1. Si n est premier, l'algorithme renvoie PREMIER.

Preuve. Si n est premier, alors les étapes 1, 3 et 5 (cf. lemme) ne peuvent pas renvoyer COMPOSÉ d'après ce qui précède. L'algorithme termine (modulo l'étape 2, étudiée dans la suite), donc il renvoie PREMIER. □

L'objectif de la suite est de montrer que si l'algorithme renvoie PREMIER, alors n est premier. Remarquons déjà que si l'algorithme renvoie PREMIER à l'étape 4, alors $n \leqslant r$ donc n est premier, car sinon 3 aurait trouvé un diviseur non trivial de n. Il suffit donc de prouver que si l'algorithme renvoie PREMIER à l'étape 6, alors n est premier.

Lemme 3.2. Si $n \geqslant 2$, alors il existe $r \leqslant \max(3, \lceil \log^5 n \rceil)$ tel que $\mathrm{pgcd}(r, n) = 1$ et $\mathrm{ord}_r(n) > \log^2 n$.

Remarque. On en déduit que pour n assez grand, on aura $r < n$, donc l'étape 4 sera inutile.

Preuve. Voir annexe. □

On reprend à présent le r minimal comme choisi à l'étape 2. Et comme on suppose que la condition de l'étape 4 n'est pas vérifiée, on a donc $n > r$. Comme $\mathrm{ord}_r(n) > 1$ (*ie* $n \not\equiv 1 \pmod r$), on en déduit qu'il existe p premier divisant n avec $\mathrm{ord}_r(p) > 1$ (*ie* $p \not\equiv 1 \pmod r$, puisque n est produit de tous ses facteurs premiers avec multiplicité).

Si $p \leqslant r$, alors $p < n$, donc 3 renverrait COMPOSÉ. Absurde. Donc $p > r$. Comme n et r sont premiers entre eux, on a $\bar{p}, \bar{n} \in U(\mathbb{Z}/r\mathbb{Z})$.
On fixe p et r dans la suite. Notons $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$. Comme l'algorithme ne renvoie COMPOSÉ dans aucune étape de la boucle Pour, on en déduit que pour tout $a \in [\![0, l]\!]$ (clair pour $a = 0$),

$$\overline{(X+a)^n} = \overline{X^n + a} \text{ dans } (\mathbb{Z}/n\mathbb{Z}[X])/(X^r - 1) \tag{3}$$

Comme $p \mid n$, on en déduit que pour tout $a \in [\![0, l]\!]$,

$$\overline{(X+a)^n} = \overline{X^n + a} \text{ dans } (\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1) \tag{4}$$

Or, par le lemme préliminaire, on a pour tout $a \in [\![0, l]\!]$,

$$\overline{(X+a)^p} = \overline{X^p + a} \text{ dans } (\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1) \tag{5}$$

Alors (4) et (5) assurent que si l'on note $n = pd$ où $d \in \mathbb{N}^*$, on a pour tout $a \in [\![0, l]\!]$,

$$\overline{X^{pd} + a} = \overline{(X+a)^{pd}} = \overline{(X^p + a)^d} \text{ dans } (\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1) \tag{6}$$

Choisissons $y \in \mathbb{N}^*$ tel que $py \equiv 1 \pmod{r}$. Alors (6) évaluée en X^y assure, puisque $X^{py} \equiv X \pmod{X^r - 1}$, que pour tout $a \in [\![0, l]\!]$,

$$\overline{X^d + a} = \overline{(X+a)^d} \text{ dans } (\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1) \tag{7}$$

Ainsi, avec (5) et (7), d et p vérifient une même propriété à laquelle on va donner un nom.

Définition 1. Pour $P \in \mathbb{Z}/p\mathbb{Z}[X]$, et $m \in \mathbb{N}^*$, on dit que m est introspectif pour P lorsque $\overline{P(X)^m} = \overline{P(X^m)}$ dans $(\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1)$.

Ainsi, $d = \frac{n}{p}$ et p sont tous deux introspectifs pour $X + a$ pour tout $a \in [\![0, l]\!]$.

Lemme 3.3. Si m et m' sont tous deux introspectifs pour $P \in \mathbb{Z}/p\mathbb{Z}[X]$, alors mm' aussi.

Preuve. On sait que $P^m - P(X^m)$ et $P^{m'} - P(X^{m'})$ sont tous deux divisibles par $X^r - 1$.
Alors $X^r - 1 \mid P^{mm'} - P(X^m)^{m'}$. Et $X^r - 1 \mid X^{mr} - 1 \mid P(X^m)^{m'} - P(X^{mm'})$. D'où $X^r - 1 \mid P^{mm'} - P(X^{mm'})$. □

Lemme 3.4. Soit $m \in \mathbb{N}^*$. Alors $\{P \in \mathbb{Z}/p\mathbb{Z}[X], m \text{ introspectif pour } P\}$ est un sous-monoïde de $(\mathbb{Z}/p\mathbb{Z}[X], \times)$.

Preuve. m est clairement introspectif pour 1 (polynôme constant). Soit $P, Q \in \mathbb{Z}/p\mathbb{Z}[X]$ avec m introspectif pour P et Q.
Alors dans $(\mathbb{Z}/p\mathbb{Z}[X])/(X^r - 1)$, on a :

$$\overline{(PQ)(X^m)} = \overline{P(X^m)Q(X^m)} = \overline{P(X)^m Q(X)^m}$$

d'où la conclusion. □

Les deux lemmes précédents impliquent que chacun des éléments de $\mathcal{I} = \{(\frac{n}{p})^i p^j, i, j \geqslant 0\}$ est introspectif pour tout élément de $\mathcal{A} = \left\{ \prod_{a=0}^{l} (X+a)^{e_a}, e_0, \ldots, e_l \geqslant 0 \right\} \subset \mathbb{Z}/p\mathbb{Z}[X]$.
Soit G l'ensemble des restes modulo r des éléments de $\mathcal{I}$. Comme $\text{pgcd}(r, n) = \text{pgcd}(r, p) = 1$, le théorème d'Euler ($n^{\varphi(r)-1} n \equiv 1 \pmod{r}$) assure que $G = \{\overline{n^i p^j}, i, j \in \mathbb{Z}\}$ est donc le sous-groupe de $U(\mathbb{Z}/r\mathbb{Z})$ engendré par $\bar{n}$ et $\bar{p}$.
Notons $t = |G|$. Comme $\text{ord}_r(n) > \log^2 n$ et $< \bar{n} > \subset G$, on a $t > \log^2 n$ ($\bullet$).
Notons $\Phi_r \in \mathbb{Z}/p\mathbb{Z}[X]$ le r-ième polynôme cyclotomique sur le corps à p élements $\mathbb{Z}/p\mathbb{Z}$ (rappelons que $p \nmid r$). Alors (cf. annexe) Φ_r est le produit de $\frac{\varphi(r)}{\text{ord}_r(p)}$ facteurs irréductibles sur $\mathbb{Z}/p\mathbb{Z}$ de degré $\text{ord}_r(p)$.
Fixons h l'un de ces facteurs irréductibles. Comme $\text{ord}_r(p) > 1$, h est de degré > 1. Posons $\mathcal{G} = \{\overline{Q}, Q \in \mathcal{A}\}$, où les classes sont dans $(\mathbb{Z}/p\mathbb{Z}[X])/(h) = F$, corps à $p^{\text{ord}_r(p)}$ éléments. De plus, $\overline{X}$ est racine de $h \in \mathbb{F}_p[X]$ irréductible de degré > 1, donc $\overline{X} \notin \mathbb{F}_p$. Donc $\overline{X}, \overline{X}+1, \ldots, \overline{X}+l$ sont des éléments non nuls de $\mathcal{G} \subset F$. Et pour $\alpha \in F^*$, on a $\alpha^{|F|-2} = \alpha^{-1}$ (Lagrange), donc

$$\mathcal{G} = \left\{ \prod_{a=0}^{l} (\overline{X}+a)^{e_a}, e_0, \ldots, e_l \geqslant 0 \right\} = \left\{ \prod_{a=0}^{l} (\overline{X}+a)^{e_a}, e_0, \ldots, e_l \in \mathbb{Z} \right\}$$

est le sous-groupe de F^* engendré par $\overline{X}, \overline{X}+1, \ldots, \overline{X}+l$.

Lemme 3.5. Soit $f, g \in \mathcal{A}$ distincts, avec $\deg f, \deg g < t$. Alors dans F, $\overline{f}$ et $\overline{g}$ sont deux éléments distincts de $\mathcal{G}$.

Preuve.

— Notons tout d'abord que comme $h \mid \Phi_r$, et que $\overline{X}$ est une racine de Φ_r dans F, on en déduit que $\overline{X}$ est une racine r-ième primitive de l'unité dans F.

— Supposons par l'absurde que $\overline{f} = \overline{g}$ dans $F = \mathbb{F}_p[X]/(h)$.
Soit $m \in \mathcal{I}$. On a donc : $\overline{f}^m = \overline{g}^m$ dans F, *ie* $\overline{f(X)^m} = \overline{g(X)^m}$. Or, m est introspectif pour f et g donc $\overline{f(X^m)} = \overline{f(X)^m}$ et $\overline{g(X^m)} = \overline{g(X)^m}$ dans $\mathbb{F}_p[X]/(X^r-1)$. Comme $h \mid X^r-1$, on a donc aussi $\overline{f(X^m)} = \overline{f(X)^m}$ et $\overline{g(X^m)} = \overline{g(X)^m}$ dans F. D'où $\overline{f(X^m)} = \overline{g(X^m)}$, *ie* $f(\overline{X}^m) = g(\overline{X}^m)$ dans F.
Donc $\overline{X}^m \in F$ est racine du polynôme $Q = f - g \in F[X]$, et ce, pour tout $m \in \mathcal{I}$. Convenons que si $m \in G$, $\overline{X}^m$ est la valeur commune des $\overline{X}^k$ pour $\bar{k} = m$ dans $\mathbb{Z}/r\mathbb{Z}$ (n'oublions pas que $\overline{X} \in F$ est racine r-ième de l'unité). Comme $\overline{X}$ est de plus primitive, si $m \neq m'$ dans G, alors $\overline{X}^m \neq \overline{X}^{m'}$ dans F sont racines de Q. Donc Q a au moins $|G| = t$ racines dans F.
Or, par choix de f et g, $\deg Q < t$. Donc $Q = 0$. C'est absurde puisque $f \neq g$ dans $\mathbb{F}_p[X]$ donc aussi dans $F[X]$.

□

Lemme 3.6. $|\mathcal{G}| \geqslant \binom{t+l}{t-1}$.

Preuve.

— Remarquons que $\bar{i} \neq \bar{j}$ dans $\mathbb{F}_p$ dès que $0 \leqslant i \neq j \leqslant l$, puisque $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor \leqslant \sqrt{r} \log n < r$, car $r > \mathrm{ord}_r(n) > \log^2 n$ ($\mathrm{ord}_r(n) \leqslant \varphi(r) < r$ comme $r > 1$), et $p > r$. Donc les éléments $\overline{X}, \overline{X}+1, \ldots, \overline{X}+l$ (où l'on confond ici l'entier et sa classe modulo p) sont deux à deux distincts dans F. Comme $\mathcal{G} \subset F^*$, on en déduit que $\overline{X}, \overline{X}+1, \ldots, \overline{X}+l$ sont $l+1$ éléments distincts non nuls de $\mathcal{G}$.

— Avec le lemme précédent, il y a dans $\mathcal{G}$ au moins autant d'éléments que dans $\mathcal{E} = \{(e_0, \ldots, e_l) \in \mathbb{N}^{l+1}, e_0 + \ldots + e_l < t\}$ (chaque $(e_0, \ldots, e_l)$ représentant la classe de $\prod_{a=0}^{l} (X+a)^{e_a}$). Or, un calcul classique montre que

$$|\mathcal{E}| = \sum_{k=0}^{t-1} \binom{k+l}{l} = \sum_{k=0}^{t-1} \left(\binom{k+l+1}{l+1} - \binom{k+l}{l+1} \right) = \binom{t+l}{t-1}$$

d'où le résultat.

□

Lemme 3.7. Si n n'est pas une puissance de p, alors $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.

Preuve. Soit $\hat{\mathcal{I}} = \{(\frac{n}{p})^i p^j, 0 \leqslant i, j \leqslant \lfloor \sqrt{t} \rfloor\} \subset \mathcal{I}$. Soit $q \neq p$ un diviseur premier de n. Alors $\nu_q((\frac{n}{p})^i p^j) = i\nu_q(n)$. Donc si $(\frac{n}{p})^i p^j = (\frac{n}{p})^{i'} p^{j'}$ alors ($\nu_q(n) \geqslant 1$) $i = i'$ donc $j = j'$. D'où $|\hat{\mathcal{I}}| = (\lfloor \sqrt{t} \rfloor + 1)^2 > t$. Comme $|G| = t$, d'après le principe des tiroirs, deux éléments de $\hat{\mathcal{I}}$, disons $m_1 > m_2$ doivent être égaux modulo r. Dans $\mathbb{F}_p[X]/(X^r-1)$, on a donc $\overline{X}^{m_1} = \overline{X}^{m_2}$.
Soit $f \in \mathcal{A}$, de sorte que m_1 et m_2 sont introspectifs pour f. Alors dans $\mathbb{F}_p[X]/(X^r-1)$, on a :

$$\overline{f(X)^{m_1}} = \overline{f(X^{m_1})} = f(\overline{X}^{m_1}) = f(\overline{X}^{m_2}) = \overline{f(X^{m_2})} = \overline{f(X)^{m_2}}$$

Comme $h \mid X^r-1$, on a aussi $\overline{f(X)}^{m_1} = \overline{f(X)}^{m_2}$ dans F. Donc $\overline{f} \in \mathcal{G} \subset F^*$ est racine du polynôme $Q = Y^{m_1} - Y^{m_2} \in F[Y]$ de degré $m_1 > 0$. Q a ainsi au moins $|\mathcal{G}|$ racines distinctes dans F, d'où $|\mathcal{G}| \leqslant m_1 \leqslant (\frac{n}{p})^{\lfloor \sqrt{t} \rfloor} p^{\lfloor \sqrt{t} \rfloor} \leqslant n^{\sqrt{t}}$. □

Théorème 3.8. Si l'algorithme renvoie PREMIER, alors n est premier.

Preuve. Remarquons d'abord que si $k \in \mathbb{N}$, alors $2^{2k+1} \leqslant (2k+2)\binom{2k+1}{k}$ donc $\binom{2k+1}{k} \geqslant \frac{2^{2k}}{k+1} > 2^{k+1}$ si $k \geqslant 4$. Donc (on le vérifie pour $k \in \{2, 3\}$) $\binom{2k+1}{k} > 2^{k+1}$ si $k \geqslant 2$ $(*)$.

On a vu précédemment qu'il suffit que traiter le cas où l'algorithme renvoie PREMIER à l'étape 6. Si $n \in \{2,3\}$, on a déjà vu que l'algorithme renvoyait PREMIER. Supposons $n \geqslant 4$. On a :

$$|\mathcal{G}| \geqslant \binom{t+l}{t-1} = \binom{t+l}{l+1} \underset{\substack{t>\sqrt{t}\log n \\ \text{par } (\bullet)}}{\geqslant} \binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{l+1} = \binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{\lfloor\sqrt{t}\log n\rfloor} \underset{\substack{l\geqslant\lfloor\sqrt{t}\log n\rfloor \text{ car} \\ t\leqslant|U(\mathbb{Z}/r\mathbb{Z})|=\varphi(r)}}{\geqslant} \binom{2\lfloor\sqrt{t}\log n\rfloor+1}{\lfloor\sqrt{t}\log n\rfloor}$$

D'où

$$|\mathcal{G}| \underset{(*)}{>} 2^{\lfloor\sqrt{t}\log n\rfloor+1} \geqslant 2^{\sqrt{t}\log n} = n^{\sqrt{t}}$$

Avec le lemme précédent, n est une puissance de p, *ie* $n = p^k$ avec $k \geqslant 1$. Si $k \geqslant 2$, alors l'algorithme aurait renvoyé COMPOSÉ à l'étape 1. Donc $k = 1$ et $n = p$ est premier. □

4 Analyse de la complexité temporelle de l'algorithme

Remarque. Les entiers que l'on sera amené à manipuler présentant *a priori* beaucoup de bits, on ne peut pas considérer l'addition par exemple comme étant une opération en temps constant. On utilisera dans la suite librement les faits suivants :

- la somme, la multiplication, la division de deux entiers de m bits se fait en $O^\sim(m)$
- le calcul du pgcd de deux entiers m et n se fait en $O^\sim(\log m \log n)$
- la somme de deux polynômes de degrés au plus d donc les coefficients sont majorés par $M > 0$ en valeur absolue se fait en $O(d \log M)$, et leur multiplication en $O^\sim(d \log M)$
- le calcul de a^b se fait en $O^\sim(b \log a)$

Théorème 4.1. La complexité temporelle asymptotique de l'algorithme est $O^\sim(\log^{21/2} n)$.

Preuve.

1. Cette étape consiste à vérifier si $n = a^b$ pour $a, b \geqslant 2$. Pour cela, il est clair que seuls les $b \leqslant \log n$ sont à envisager. L'idée générale est que pour chacun des b envisageables, on mène une recherche dichotomique dans $[\![2, n]\!]$ pour chercher un éventuel a tel que $a^b = n$. Pour un b donné, il y a au plus $\log n$ étapes. En comptant les exponentiations à réaliser, on a $O^\sim(\log^3 n)$ opérations à b fixé, donc $O^\sim(\log^4 n)$ au total.
2. On cherche ici un entier r tel que $\mathrm{ord}_r(n) > \log^2 n$. Ceci peut être fait en essayant les valeurs successives de r et en vérifiant si $n^k \not\equiv 1 \pmod r$ pour tout $1 \leqslant k \leqslant \log^2 n$. Pour un r fixé, cela impliquera $\log^2 n$ multiplications et divisions euclidiennes par r, donc $O^\sim(\log^2 n \log^2 r)$, et un calcul de pgcd en $O^\sim(\log n \log r)$. Comme seules les valeurs de r inférieures à $\lceil \log^5 n \rceil$ doivent être examinées, on a donc au total $O^\sim(\log^7 n)$.
3. On doit calculer $\mathrm{pgcd}(a, n)$ pour $a \in [\![1, r]\!]$ qui prennent chacun un temps $O^\sim(\log n \log r) = O^\sim(\log n)$. Au total, cela fait $O^\sim(r \log n) = O^\sim(\log^6 n)$.
4. Cette étape est simplement en $O(\log n)$ car $\log r = O(\log n)$.
5. On doit enfin vérifier $l = O(\sqrt{r}\log n) = O(\log^{7/2} n)$ égalités. Avec l'exponentiation rapide, chacune de ces égalités requiert $O(\log n)$ multiplications modulo $X^r - 1$ et modulo n de polynômes, donc il faut $O^\sim(r \log^2 n) = O^\sim(\log^7 n)$ opérations. On a donc une complexité en $O^\sim(\log^{21/2} n)$, qui domine toutes les autres.

□

5 Annexe

5.1 Preuves des lemmes préliminaires

Preuve du lemme 2.2. Notons $d_n = \underset{1\leqslant i\leqslant n}{\mathrm{ppcm}}\, i$, et $I_{m,n} = \int_0^1 x^{m-1}(1-x)^{n-m}dx$ pour $m \in [\![1, n]\!]$.

Alors d'une part, il vient en développant que $I_{m,n} = \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} \frac{1}{k+m}$. Par conséquent, $d_n I_{m,n}$ est un entier. Comme $I_{m,n} > 0$, on a donc $d_n I_{m,n} \in \mathbb{N}^*$.

D'autre part, une intégration par parties montre que si $m \in [\![1, n-1]\!]$, alors $I_{m+1,n} = \frac{m}{n-m} I_{m,n}$. Par récurrence finie immédiate, on en déduit que

$$I_{m,n} = \frac{(m-1)\dots 1}{(n-m+1)\dots(n-1)} I_{1,n} = \frac{(m-1)!(n-m)!}{n!} = \frac{1}{m\binom{n}{m}}$$

De ces deux observations, on en déduit que $m\binom{n}{m} \mid d_n$ pour tout $m \in [\![1, n]\!]$. En particulier, comme $(2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n+1}$, on a que $n\binom{2n}{n} \mid d_{2n} \mid d_{2n+1}$, et $(2n+1)\binom{2n}{n} \mid d_{2n+1}$. D'où ($n$ et $2n+1$ sont premiers entre eux), $n(2n+1)\binom{2n}{n} \mid d_{2n+1}$, donc $d_{2n+1} \geqslant n4^n$, puisque $(2n+1)\binom{2n}{n} \geqslant \sum_{k=0}^{2n} \binom{2n}{k} = 4^n$. Donc pour $n \geqslant 2$, $d_{2n+1} \geqslant 2^{2n+1}$. Et pour $n \geqslant 4$, $d_{2n+2} \geqslant d_{2n+1} \geqslant n2^{2n} \geqslant 2^{2n+2}$. Donc le lemme est vrai pour $n \geqslant 9$ et pour $n = 7$. Il suffit alors de le vérifier pour $n = 8$. Or, $d_8 = 8 \times 7 \times 5 \times 3 = 840 \geqslant 256$. Ceci conclut. □

Preuve du lemme 3.2. C'est vrai si $n = 2$ ($r = 3$ convient), si $n = 3$ ($r = 5$ convient) et si $n = 4$ ($r = 11$ convient). On suppose donc que $n \geqslant 5$, de sorte que $B = \lceil \log^5 n \rceil > 10$.

— Il est clair que $\max\{k \in \mathbb{N}, \exists m \geqslant 2, m^k \leqslant B\} = \lfloor \log B \rfloor$ (on rappelle qu'il s'agit toujours du logarithme en base 2).

— Soit $A = n^{\lfloor \log B \rfloor} \prod_{i=0}^{\lfloor \log^2 n \rfloor} (n^i - 1)$, et soit $r \geqslant 2$ le plus petit entier qui ne divise pas A. Alors

$$A < n^{\lfloor \log B \rfloor + \frac{1}{2}\log^2 n(\log^2 n+1)} \underset{(\circ)}{\leqslant} n^{\log^4 n} = 2^{\log^5 n} \leqslant 2^B \tag{8}$$

où $(\circ)$ vient du fait que

$$\lfloor \log B \rfloor + \frac{1}{2}\log^2 n(\log^2 n + 1) \underset{n \geqslant 5}{\leqslant} \log(\log^5 n + 1) + \frac{1}{2}\log^4 n + \frac{1}{10}\log^4 n \leqslant \log^4 n$$

puisqu'on vérifie que $\log(\log^5 n + 1) \leqslant \frac{2}{5}\log^4 n$ si $n \geqslant 5$.

— Si par l'absurde $r > B$, alors A est divisible par $1, 2, \dots, B$, donc par $\operatorname{ppcm}_{1 \leqslant i \leqslant B} i \geqslant 2^B$. Ceci contredit le fait que $2 \leqslant A < 2^B$ avec (8). Donc $r \leqslant B = \lceil \log^5 n \rceil$.

— Montrons que r et n sont premiers entre eux. On sait que $r \nmid A$, donc il existe p premier divisant r avec $\nu_p(r) > \nu_p(A)$. Comme $r \leqslant B$, on a nécessairement $\nu_p(r) \leqslant \lfloor \log B \rfloor$ avec le premier point. Et si par l'absurde p divisait aussi n, alors comme $n^{\lfloor \log B \rfloor} \mid A$, on aurait $\nu_p(A) \geqslant \lfloor \log B \rfloor \geqslant \nu_p(r)$. Contradiction. Donc $p \nmid n$, et ainsi, $p^{\nu_p(r)} \mid \frac{r}{\operatorname{pgcd}(n,r)}$. Comme $\nu_p(r) > \nu_p(A)$, on a que $\frac{r}{\operatorname{pgcd}(n,r)}$ ne divise pas non plus A. Donc par définition de r, $\frac{r}{\operatorname{pgcd}(n,r)} \geqslant r$, d'où $\operatorname{pgcd}(n, r) = 1$.

— Enfin, pour tout $i \in [\![1, \lfloor \log^2 n \rfloor]\!]$, $r \nmid n^i - 1$, donc $\operatorname{ord}_r(n) > \log^2 n$, ce qui conclut.

□

5.2 Autour des extensions de corps

Théorème 5.1. Soit F un surcorps de K (corps). Soit $\theta \in F$ algébrique de degré n sur K, et soit $\pi_\theta \in K[X]$ le polynôme minimal de θ sur K. Alors :

1. π_θ est irréductible sur K
2. $K(\theta)$ (sous-corps de F engendré par θ et K) coïncide avec l'algèbre $K[\theta]$ des polynômes en θ à coefficients dans K, qui est donc un corps de dimension n sur K, isomorphe à $K[X]/(\pi_\theta)$
3. Si $\alpha \in F$, α est algébrique sur K si et seulement si $K[\alpha]$ est de dimension finie sur K.

Définition 2. Une extension L d'un corps K est dite :

— *finie* lorsque L est de dimension finie sur K

— *algébrique* lorsque tout $\theta \in L$ est algébrique sur K

— *simple* lorsqu'il existe $\theta \in L$ tel que $L = K(\theta)$

Théorème 5.2.

1. Si $P \in K[X]$ est irréductible sur K, alors il existe une extension simple algébrique sur K engendrée par une racine de P et K.
2. De plus, si L, L' sont des extensions de K, et $(\alpha, \beta) \in L \times L'$ avec $P(\alpha) = P(\beta) = 0$, on a : $K(\alpha) \underset{\text{corps}}{\simeq} K(\beta)$.

Définition 3. Soit F une extension de K, et $P \in K[X] \setminus K$. On dit que F est *un* corps de décomposition de P lorsque P est scindé sur F de racines $\alpha_1, \ldots, \alpha_n \in F$, et que $F = K(\alpha_1, \ldots, \alpha_n)$.

L'utilisation itérée du théorème précédent permet de prouver le suivant.

Théorème 5.3. Si K est un corps, et $P \in K[X] \setminus K$, alors il existe un corps de décomposition de P sur K. De plus, deux corps de décomposition de P sur K sont isomorphes en tant que K-algèbres.

5.3 Sur les corps finis

On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments.

Théorème 5.4. Soit F un corps fini. Alors avec $p = \operatorname{car} K$, F devient un surcorps fini de son sous-corps premier $\mathbb{F}_p$, donc $|F| = p^n$, où $n = [F : \mathbb{F}_p]$.

Théorème 5.5 (Existence et unicité des corps finis)**.** Pour tout nombre premier p et tout $n \in \mathbb{N}^*$, il existe un unique corps fini à p^n éléments (à isomorphisme près), noté $\mathbb{F}_{p^n}$. Chacun d'entre eux est isomorphe au corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, où $q = p^n$.

Théorème 5.6 (Sous-corps d'un corps fini)**.** Soit $\mathbb{F}_q$ le corps fini à $q = p^n$ éléments. Alors :

1. Tout sous-corps de $\mathbb{F}_q$ a un cardinal p^m où $m \mid n$.
2. Réciproquement, si $m \mid n$, alors il existe un unique sous-corps de $\mathbb{F}_q$ de cardinal p^m, qui est le corps décomposition de $X^{p^m} - X$ sur $\mathbb{F}_p$ (et qui coïncide de plus avec l'ensemble des racines de $X^{p^m} - X$ dans $\mathbb{F}_q$).

5.4 Polynômes cyclotomiques sur les corps finis

Définition 4. Soit $n \in \mathbb{N}^*$, et K un corps. Le corps de décomposition du polynôme $X^n - 1$ sur K est appelé le n-ième corps cyclotomique sur K, et est noté $K^{(n)}$. Les racines de $X^n - 1$ dans $K^{(n)}$ sont appelées les racines n-ièmes de l'unité sur K, et l'ensemble de ces racines est noté $E^{(n)}$.

Théorème 5.7. Soit $p = \operatorname{car} K$. On suppose ici et dans la suite que $p \nmid n$. Alors $(E^{(n)}, \times)$ est un groupe cyclique d'ordre n. Tout générateur de ce groupe cyclique est appelé racine n-ième *primitive* de l'unité. Il y en a au total $\varphi(n)$.

Preuve. Soit $P = X^n - 1 \in K[X]$. Alors $P' = nX^{n-1}$ est scindé sur K et ne possède que 0 comme racine (car $p \nmid n$), qui n'est pas racine de P. Donc P et P' sont premiers entre eux dans $K[X]$, et aussi dans $K^{(n)}[X]$ par invariance du pgcd par extension de corps. Donc P est scindé à racines simples dans $K^{(n)}$, et $|E^{(n)}| = n$. On vérifie aisément que $(E^{(n)}, \times)$ est un sous-groupe fini de $(K^{(n)*}, \times)$, donc est cyclique. □

Définition 5. On suppose toujours que $p \nmid n$. Alors $\Phi_n = \prod_{\substack{\eta \in E^{(n)} \\ \eta \text{ primitive}}} (X - \eta)$ est appelé le n-ième polynôme cyclotomique sur K.

Proposition 5.8. Si $p = \operatorname{car} K \nmid n$, alors :

1. $X^n - 1 = \prod_{d \mid n} \Phi_d$ (si $p \nmid n$ et $d \mid n$ alors $p \nmid d$)
2. Les coefficients de Φ_n sont dans le sous-corps premier de K.

Preuve.

1. Chaque racine n-ième de l'unité est une racine d-ième primitive de l'unité pour exactement un diviseur d de n.

2. Récurrence forte sur n, en utilisant l'unicité de la division euclidienne dans $K^{(n)}[X]$

□

Théorème 5.9. On suppose ici que $K = \mathbb{F}_q$ avec $q = p^k$ $(k \geqslant 1)$. On suppose toujours que $p \nmid n$. Alors Φ_n se factorise en $\frac{\varphi(n)}{d}$ polynômes irréductibles unitaires de $K[X]$, de même degré $d = \mathrm{ord}_n(q)$.

Preuve. On rappelle que si $l \in \mathbb{N}^*$, les éléments de $\mathbb{F}_{q^l}$ surcorps de $\mathbb{F}_q$ sont exactement les racines de $X^{q^l} - X$ dans une extension qui scinde ce polynôme. Soit η une racine n-ième primitive de l'unité sur K. Alors si $l \in \mathbb{N}^*$,

$$\eta \in \mathbb{F}_{q^l} \iff \eta^{q^l} = \eta \iff q^l \equiv 1 \pmod{n}$$

Comme le plus petit entier pour lequel ceci soit vrai est d, on en déduit que $\eta \in \mathbb{F}_{q^d}$, mais $\eta \notin \mathbb{F}_{q^l}$ pour tout $l \in [\![1, d-1]\!]$. Ainsi,

$$K^{(n)} = K(\eta, \eta^2, \ldots, \eta^{n-1}) = K(\eta) = \mathbb{F}_{q^d}$$

(l'inclusion $\supset$ venant du fait que $K(\eta)$ ne peut être aucun des $\mathbb{F}_{q^l}$ pour $l \in [\![1, d-1]\!]$). Donc le degré d'algébricité de η sur K est $d = [\mathbb{F}_{q^d} : \mathbb{F}_q]$. Ainsi, le polynôme minimal de η sur K, $\pi_{\eta,K}$, divise Φ_n dans $K[X]$ et est irréductible sur K. En considérant $\frac{\Phi_n}{\pi_{\eta,K}} \in K[X]$ et en répétant l'opération, on obtient le résultat voulu. □

5.5 Implémentation

5.5.1 Le code Python

On suit exactement la démarche décrite dans l'analyse de la complexité temporelle, en utilisant le plus possible les fonctions qui existent déjà dans Python.

```
from math import floor, log, gcd
from numpy import polynomial
def perfect_pow(n): # Renvoie True si et seulement si n=1 ou si n
#est une puissance parfaite
    if n == 1: return True
    b = 2
    while 2**b <= n:
        x, y = 1, n + 1
        while y - x > 1:
            a = (x + y) // 2
            if a**b > n:
                y = a
            else:
                x = a
        if x**b == n:
            return True
        b += 1
    return False

def reduce(A, n, r): # reduit A dans (Z/nZ[X])/(X^r-1)
    P = A.coef
    Q = [0] * r
    l = len(P)
    for i in range(r):
        Q[i] = sum(P[k] for k in range(i, l, r)) % n
    return polynomial.Polynomial(Q)

def fast_exp(p, m, n, r): # p est un polynome, et la fonction calcule p^m
#dans (Z/nZ[X])/(X^r-1)
    if m == 0:
```

```
        return polynomial.Polynomial([1] + [0] * (r - 1))
    q = fast_exp(p, m//2, n, r)
    q1 = reduce(q**2, n, r)
    if m%2 == 0:
        return q1
    return reduce(q1*p, n, r)

def step5(n, r): # renvoie True si (X + a)^n = X^n + a dans (Z/nZ[X])/(X^r-1) pour
#tout a entre 1 et l, et False sinon
    l = floor(phi(r)**0.5*log(n)/log(2))
    for a in range (1, l + 1):
        if fast_exp(reduce(polynomial.Polynomial([a, 1]), n, r), n, n, r)
        != reduce(polynomial.Polynomial([a] + [0] * (n - 1) + [1]), n, r):
            return False
    return True

def find_r(n): # trouve le plus petit r de l'étape 2
    r = 2
    while True:
        if gcd(r, n) == 1:
            k, boo, p = 1, True, n%r
            while boo and 2**(k**0.5) <= n:
                if p == 1:
                    boo = False
                p = (n*p)%r
                k += 1
            if boo: return r
        r += 1

def phi(n):
    a = 1
    for i in range (2, n):
        if gcd(n, i) == 1:
            a += 1
    return a

def aks(n): # Renvoie True si et seulement si n est premier
    if perfect_pow(n): return False
    r = find_r(n)
    for a in range (2, r + 1):
        d = pgcd(a, n)
        if d > 1 and d < n:
            return False
    if n <= r: return True
    return step5(n, r)
```

5.5.2 Quelques remarques pratiques

L'exécution du programme ci-dessus est en réalité décevante. Les durées d'exécution sont rassemblées dans le tableau ci-dessous.

Entier	2	11	101	1009	5003	10 007	50 021	100 003	500 009	1 000 003
Durée (s)	10^{-5}	10^{-4}	0.1	0.5	1.3	2	6.4	11.4	60.2	121

L'explication est simple. Bien que l'algorithme AKS soit de manière révolutionnaire en temps polynomial, son

nombre d'opérations est supérieur à $\log^{21/2} n$. On peut vérifier grossièrement qu'il faut que n soit au moins de l'ordre de 10^{40} pour que $\log^{21/2} n$ ne soit pas trop grand par rapport à $\sqrt{n}$ (le logarithme étant toujours pris en base 2). Or, les ordinateurs actuels ne peuvent clairement pas traiter un nombre d'opérations de l'ordre de 10^{20} en temps raisonnable, ce qui explique l'inefficacité pratique de l'algorithme (à moins que les ordinateurs quantiques ne voient le jour !).

Remarque. Depuis l'article original, de nombreux autres chercheurs ont amélioré l'algorithme AKS. Certains ont réussi à construire un algorithme de test de primalité déterministe en $O^{\sim}(\log^6 n)$, mais la preuve de leur complexité requiert de la théorie analytique des nombres...

6 Références bibliographiques

[1] M. Agrawal, N. Kayal, et N. Saxena, *PRIMES is in P*, 2002

[2] M. Nair, *On Chebyshev-type inequalities for primes*, 1982

[3] R. Lidl et H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986

[4] Joachim von zur Gathen et Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999