Théorème d'AKS

OUMZIL Ziad Eddine

10 juin 2021

Résumé

On étudie un algorithme déterministe de complexité polynômiale ($O(log(n)^{\frac{21}{2}})$) qui détermine si un entier est premier ou non.

1 Introduction

Ce TIPE a été l'objet d'une étude commune avec KHAIR MOHAMED et est largement inspiré de l'article "PRIMES is in P" de trois scientifiques indiens MANINDRA AGRAWAL, NEERAJ KAYAL, et NITIN SAXENA (AKS) .

Les tests de primalité sont centraux en cryptographie. En effet, l'algorithme RSA 1977 repose sur la donnée de deux nombres premiers suffisamment grand pour que, connaissant uniquement la valeur de leur produit, arriver à décomposer cette valeur en facteurs premiers soit délicat.L'algorithme AKS est un exemple de test de primalité qui s'exécute en temps polynomial et qui de plus est déterministe. Dans ce TIPE, on s'intéresse à la preuve de ce théorème : je commence dans la première partie par démontrer certains résultats dont j'aurai besoin pour la suite. Et en deuxième partie, on va étudier le théorème d'AKS ainsi que sa preuve.

Notations :

- On note Z_n l'anneau des entiers modulo n ($n \in N$).
- F_p est le corps lorsque p est premier
- Si $f(X)$, $g(X)$ et $P(X)$ sont trois fonctions polynomiales de K[X] et $n \in N^*$, alors l'écriture

$$f(X) = g(X)\ mod(P(X), n)$$

  est équivalente à $\exists Q, R \in K[X]\ f(X) = g(X) + Q(X)P(X) + nR(X)$
- Pour $r, n \in N$ tels que $pgcd(r, n) = 1$, $o_r(n)$ représente l'ordre de n modulo r (ie $o_r(n)$ le plus petit entier non nul k tel que $n^k \equiv 1\ [r]$)
- $\phi(r)$ l'indicatrice d'euler.
- $\phi_r(X)$ le r-ième polynôme cyclotomique.
- On note d_n l'entier tel que $d_n = ppcm(1, 2, \cdots, n)$
- Si p est premier, $v_p(n)$ est le plus grand entier k tel que $p^k \mid n$

1.1 Premiers résultats

Lemme 1.1. *Soient $n \geq m$ deux entiers non nuls, on a*

$$m \cdot \binom{n}{m} \mid d_n$$

Démonstration. Soit p un nombre premier. Notons $a_n = \lfloor \log_p(n) \rfloor$ alors il est évident que $v_p(d_n) = a_n$. Et par la formule de Légendre on a : $v_p(m \cdot \binom{n}{m}) = v_p(m) + \sum_{k=1}^{\infty}(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{m}{p^k} \rfloor\ - \lfloor \frac{n-m}{p^k} \rfloor)$ donc

$$v_p(m \cdot \binom{n}{m}) = v_p(m) + \sum_{k=1}^{a_n}(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{m}{p^k} \rfloor\ - \lfloor \frac{n-m}{p^k} \rfloor)$$

si $i = v_p(m)$ alors $\forall k \in [|1, i|]\ \lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{m}{p^k} + \frac{n-m}{p^k} \rfloor = \lfloor \frac{m}{p^k} \rfloor\ + \lfloor \frac{n-m}{p^k} \rfloor$ (car $\frac{m}{p^k} \in N$)
sinon on a l'inégalité suivante $\lfloor \frac{n}{p^k} \rfloor \leq \lfloor \frac{m}{p^k} \rfloor\ + \lfloor \frac{n-m}{p^k} \rfloor + 1$

d'où

$$v_p(m \cdot \binom{n}{m}) = i + \sum_{k=i+1}^{a_n} (\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{m}{p^k} \rfloor \ - \lfloor \frac{n-m}{p^k} \rfloor) \leq i + \sum_{k=i+1}^{a_n} 1 = a_n$$

□

Lemme 1.2. *Soit n un entier naturel supérieur à 9*

$$d_n \geq 2^n$$

Démonstration. Par le lemme 1.1 $(2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n+1} \mid d_{2n+1}$ et $n\binom{2n}{n} \mid d_{2n} \mid d_{2n+1}$
n et $2n+1$ étant premiers entre eux donc

$$n(2n+1)\binom{2n}{n} \mid d_{2n+1}$$

$$\begin{aligned} d_{2n+1} &\geq n(2n+1)\binom{2n}{n} \\ &\geq n2^{2n} \\ &\geq 2^{2n+1} \quad \text{si } n \geq 2 \end{aligned}$$

$d_{2n+2} \geq d_{2n+1} \geq n2^{2n} \geq 2^{2n+2}$ si $n \geq 4$

On en déduit que $\forall n \geq 9 \ \ d_n \geq 2^n$ □

le résultat suivant a une importance majeure dans ce qui suit.

Lemme 1.3. *Soit $n \geq 2$ entier, il existe $r \leq max(3, \lfloor log(n)^5 \rfloor)$ tel que $o_r(n) > log(n)^2$*

Démonstration. Inspirée de [2].
Pour n = 2,3,4 c'est vrai

Si $n \geq 5$ alors $\lceil log^5(n) \rceil \geq 9$, on pose $\alpha = \lceil log^5(n) \rceil$

On a

$$\begin{aligned} A = n^{\lfloor log(\alpha) \rfloor} \cdot \prod_{i=1}^{\lfloor log^2(n) \rfloor} (n^i - 1) &< n^{\lfloor log(\alpha) \rfloor + \frac{1}{2} \lfloor log^2(n) \rfloor (\lfloor log^2(n) \rfloor + 1)} \\ &\leq n^{\frac{1}{2}(log(n)^4 + log(n)^2 + 10log(n))} = n^{log(n) \cdot P(log(n))} \\ &< n^{log^4(n)} \text{ car si } n \geq 5 \ P(log(n)) \leq log(n)^3 \\ &= 2^{log(n)^5} \end{aligned}$$

par le lemme 1.2

$$A < 2^{log(n)^5} \leq d_{\lfloor log^5(n) \rfloor}$$

il existe donc $h < log^5(n)$ tel que h ne divise pas $n^{\lfloor log(\alpha) \rfloor} \cdot \prod_{i=1}^{\lfloor log^2(n) \rfloor} (n^i - 1)$

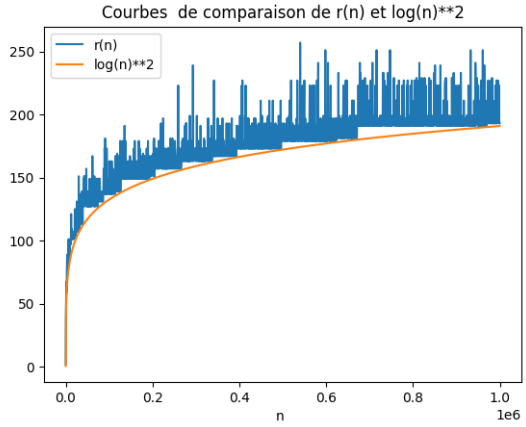
On remarque aussi que si p est un diviseur premier de n alors

$$\begin{aligned} v_p(A) &= \lfloor log(\alpha) \rfloor v_p(n) \\ &\geq \lfloor log(\alpha) \rfloor \\ &\geq \lfloor log_p(\alpha) \rfloor = max_{2 \leq r \leq \alpha} v_p(r) \\ &\geq v_p(h) \end{aligned}$$

Comme h ne divise pas A , alors il existe r un diviseur de h tel que $r \wedge n = 1$
r ne divise pas A alors $o_r(n) > \lfloor log^2(n) \rfloor$. □

On considérera dans ce qui suit un tel r **minimal**.

Remarque. *Si on admet la conjecture d'Artin ou celle de Sophie Germain, on peut déduire l'existence d'un tel r tel que* $r = O(log^2(n))$ *(Voir [1])*



Lemme 1.4. *Si p est un nombre premier alors* $\forall a \in N$

$$(X+a)^p = X^p + a \mod(p)$$

Démonstration. C'est un résultat direct de la propriété suivante :

$$p \mid \binom{p}{k} \text{ si } 1 \leq k \leq p-1$$

□

Corollaire 1.4.1. *Si p est un nombre premier alors* $\forall a \in N$

$$(X+a)^p = X^p + a \mod(X^r - 1, p)$$

Definition 1.1 (Raçines primitives de l'unité)**.** Pour r un entier naturel, ζ est dite est une racine primitive r-ème de l'unité si et seulement si $\zeta^r = 1$ et $\forall k < r \ \zeta^k \neq 1$

Remarque. *Si* ζ *est une raçine primitive r-ième de l'unité sur un corps K alors l'ensemble des raçines primitives r-ième de l'unité est* $S_r = \{\zeta^k \mid pgcd(k,r) = 1 \text{ et } k < r\}$ *et* $Card(S_r) = \phi(r)$.

Definition 1.2 (polynômes cyclotomique)**.** Pour r un entier naturel. On définit $\phi_r(X)$ le r-ème polynome cyclotomique par :

$$\phi_r(X) = \prod_{\zeta \in S_r} (X - \zeta)$$

Propriétés

1. $\deg(\phi_r(X)) = \phi(r)$
2. $X^r - 1 = \prod_{d|r} \phi_d(X)$
3. $\phi_r(X)$ est dans $K[X]$, si le corps de base est K
4. $\phi_r(X) \in Z[X]$ Si le corps de base est Q

Démonstration. Montrons 4 par récurrence forte : c'est vraie pour $r = 1$
Soit $r > 1$, supposons que la propriété est vraie pour tout $k < r$ Ainsi

$$X^r - 1 = \phi_r(X) \cdot \prod_{d|r, d<r} \phi_d(X) = \phi_r(X) \cdot P(X)$$

Par hypothèse de récurrence $P(X)$ est un polynome unitaire de $Z[X]$
On a imédiatemment que $\phi_r(X)$ est dans $Q[X]$, il existe donc un entier q tel que $q\phi_r(X)$ soit dans $Z[X]$.

$$qX^r - q = (q\phi_r(X)) \cdot P(X)$$

On introduit la notation $c(Q)$ étant le pgcd des coefficients de Q, pour $Q \in Z[X]$
D'après le lemme de Gauss, c est multiplicative.

$$\begin{aligned} c(qX^r - q) &= c((q\phi_r(X)) \cdot P(X)) \\ &= c(q\phi_r(X)) \times c(P(X)) \\ &= c(q\phi_r(X)) \text{ car P est unitaire} \end{aligned}$$

donc $c(q\phi_r(X)) = q$ d'où $\phi_r(X) = \frac{q\phi_r(X)}{q} \in Z[X]$ □

Lemme 1.5. *Soient p un nombre premier, et $h(X)$ un polynôme irréductible sur le corps $F_p[X]$, alors l'anneau $F_p[X]/h(X)$ est un corps fini de cardinal $p^{deg(h)}$*

Démonstration. Si $P(X)$ est un élément de $F_p[X]/h(X)$ non nul, alors $h(X)$ ne divise pas $P(X)$ sur le corps $F_p[X]$, $h(X)$ étant irréductible alors les deux polynômes sont premiers entre eux sur le corps $F_p[X]$. Par le théorème de bezout, il existe U,V $\in F_p[X]$ tel que $U \cdot P + V \cdot h = 1$ dans F_p
D'où l'existence de U $\in F_p[X]/h(X)$ tel que $U \cdot P = 1$
Si d=deg(h), alors l'application linéaire qui pour un élément de F_p^d associe le polynome sur $F_p[X]/h(X)$ est un isomorphisme. □

Lemme 1.6. *Soit $r > 1$ et p un nombre premier, alors $\phi_r(X)$ le r-ièmes polynôme cyclotomique sur $F_p[X]$ s'écrit comme le produit de polynômes irréductibles de degré $o_r(p)$.*

Démonstration. Inspirée de [3] : Soit h(X) un tel facteur irréductible sur $F_p[X]$ de degré d. On travaille dans le corps fini $K = F_p[X]/h(X)$. comme $h(X)$ divise $\phi_r(X)$ alors $\phi_r(X) \equiv 0$ sur K donc X est une raçine primitive r-ième de l'unité sur K. K est de cardinal p^d alors $X^{p^d-1} \equiv 1$. On en déduit que $r \mid p^d - 1$ donc $o_r(p) \mid d$.
Puisque X est une raçine primitive r-ième de l'unité sur K, alors K est engendré par ses raçines qui appartiennent au corps K', K' étant corps de décomposition de $X^{p^d} - 1$ sur $F_p[X]$ de cardinal $p^{o_r(p)}$[4].
K est donc un sous corps de K' d'où $p^d \leq p^{o_r(p)}$. On en déduit que $d = o_r(p)$ □

2 Algorithme d'AKS

Étant donné un entier n .

1. Verifier que n n'est pas une puissance d'un entier.
2. Chercher $1 \leq r \leq \lceil log^5(n) \rceil$ minimal tel que $o_r(n) > log^2(n)$
3. Verifier que $k \wedge n = 1$ pour $k < r$
4. Verifier pour $1 \leq a \leq \lfloor \sqrt{\phi(r)} log(n) \rfloor$

$$(X + a)^n = X^n + a \ mod(X^r - 1, n)$$

Théorème 2.1 (theorème d'AKS)**.** *les quatres étapes sont verifiées si et seulement si n premier*

Remarque. *Par le corollaire 1.4.1 et le lemme 1.3, On a immédiatement la réciproque.*

À présent on suppose que les 4 étapes sont vérifiées, et on suppose par absurde que n n'est pas premier. Soit p un diviseur premier de n. L'étape 3 implique que p¿r .
Notons $l = \lfloor \sqrt{\phi(r)} log(n) \rfloor$, on a pour tout a $\leq l$

$$(X+a)^n = X^n + a \ mod(X^r - 1, n)$$

donc

$$(X+a)^n = X^n + a \ mod(X^r - 1, p)$$

On déduit que

$$(X+a)^{\frac{n}{p}} = X^{\frac{n}{p}} + a \ mod(X^r - 1, p) \tag{1}$$

Par le corollaire 1.4.1

$$(X+a)^p = X^p + a \ mod(X^r - 1, p) \tag{2}$$

Definition 2.1. Soient $f(X)$ un polynôme et m un entier, on dit que m est introspectif pour f si

$$f(X)^m = f(X^m) \ mod(X^r - 1, p)$$

Remarque. *d'après (1) et (2),* $\frac{n}{p}$ *et* p *sont introspectifs pour* $f(X) = X + a$ *pour tout* $0 \leq a \leq l$

Propriétés

1. si m et m' sont introspectifs pour $f(X)$, alors $m \cdot m'$ l'est aussi.
2. si m est introspectif pour f(X) et g(X), alors m est introspectif pour fg

Démonstration. □

On en déduit que tous les éléments de $I = \{p^i(\frac{n}{p})^j \mid i, j \geq 0\}$ sont introspectifs pour les éléments de $L = \{\prod_{a=0}^{l}(X+a)^{e_a} \mid e_a \geq 0\}$.

On considère G le sous groupe multiplicatif de Z_r^* constitué des éléments de I modulo r ($n \wedge r = 1$), et notons $t = |G|$. Soient $h(X)$ un facteur irréductible qui divise $\phi_r(X)$ et $K = F_p[X]/h(X)$. Soit H l'ensemble L sur K, H est un sous groupe multiplicatif du corps K .

Lemme 2.2.

$$t = |G| > log^2(n)$$

Démonstration. $n^{|G|} = 1 \ mod(r)$ donc $|G| > o_r(n) > log^2(n)$ □

Lemme 2.3.

$$|H| \geq \binom{t+l}{l+1}$$

Démonstration. (inspirée de [2]) On cherche à montrer que si $f(X)$ et $g(X)$ sont deux éléments distincts de l'ensemble L et de degré inférieure à t-1, sont envoyés vers des éléments différents de H.
Si $f(X) \equiv g(X)$ sur K, alors pour tout $m \in G$ $f(X)^m \equiv g(X)^m$ sur K, m est introspectif pour f et g. Donc

$$f(X^m) \equiv g(X^m) \text{ sur } K$$

Donc X^m est une raçine du polynôme $Q(Y) = f(Y) - g(Y) \ \ \forall m \in G$
Comme l'a été déjà mentionné précédemment (voir preuve du lemme 1.6), X est une racine primitive r-ième de l'unité sur K, et puisque $n \wedge r = 1$ alors $m \wedge r = 1$ donc les $(X^m)_{m \in G}$ sont distincts Ainsi $Q(Y)$ admet t raçine sur le corps K, alors que son degré est au plus $t - 1$, ce qui est absurde.

$X, X+1, X+2, ..., X+l$ sont des éléments distincts de H ($l = \lfloor \sqrt{\phi(r)} log(n) \rfloor < \sqrt{r \cdot r} = r < p$)
Donc les polynômes $\prod_{a=0}^{l}(X+a)^{e_a}$ tels que $\sum_{a=0}^{l} e_a \leq t - 1$ sont des éléments distincts de H, il en existe $\binom{t+l}{l+1}$ de tels polynômes. □

Corollaire 2.3.1.

$$|H| > n^{\sqrt{t}}$$

Démonstration.

$$\begin{aligned}
|H| &\geq \binom{t+l}{l+1} \\
&> \binom{\lfloor\sqrt{t}\cdot log(n)\rfloor + l}{l+1} \text{ Car } t > \sqrt{t}\cdot log(n) \\
&\geq \binom{2\cdot\lfloor\sqrt{t}\cdot log(n)\rfloor}{\lfloor\sqrt{t}\cdot log(n)\rfloor + 1} \text{ Car } l = \lfloor\sqrt{\phi(r)}\cdot log(n)\rfloor > \sqrt{t}\cdot log(n) \\
&= \frac{m}{(m+1)(2m+1)}\binom{2m}{m} \text{ Avec } m = \lfloor\sqrt{t}\cdot log(n)\rfloor \\
&\geq \frac{m}{(m+1)(2m+1)}2^{2m} \\
&\geq 2^{(m+1)} \\
&\geq 2^{\sqrt{t}\cdot log(n)} = n^{\sqrt{t}}
\end{aligned}$$

□

Lemme 2.4. *Puisque n n'est pas une puissance d'un entier alors*

$$|H| < n^{\sqrt{t}}$$

Démonstration. (inspirée de [1]) le sous ensemble $A = \{(\frac{n}{p})^i \cdot p^j \mid 0 \leq i, j \leq \lfloor\sqrt{t}\rfloor\}$ de G contient $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ distincts entiers (car n n'est pas une puissance).
donc il 'existe m et m' dans A, avec $m > m'$ de même congruence modulo r.
d'où

$$X^m = X^{m'}\ mod(X^r - 1)$$
$$X^m = X^{m'}\ mod(h(X))$$

Soit $f(X) \in H$

$$\begin{aligned}
f(X)^m &= f(X^m)\ mod(h(X), p) \\
&= f(X^{m'})\ mod(h(X), p) \\
&= f(X)^{m'}\ mod(h(X), p)
\end{aligned}$$

On en déduit que $f(X)$ est une raçine du polynome $Q(Y) = Y^m - Y^{m'}$, qui est de degré $m \leq (\frac{n}{p})^{\lfloor\sqrt{t}\rfloor}\cdot p^{\lfloor\sqrt{t}\rfloor}$. Il en découle $|H| < n^{\sqrt{t}}$ □

Conclusion :
D'après le lemme 2.4 et 2.3, on obtient une contardiction. Ce qui montre que n **est premier**

3 Compléxité :

On reprend l'algorithme d'AKS

1. Verifier que n n'est pas une puissance d'un entier.
2. Chercher $1 \leq r \leq \lceil log^5(n)\rceil$ minimal tel que $o_r(n) > log^2(n)$
3. Verifier que $k \wedge n = 1$ pour $k < r$
4. Verifier pour $1 \leq a \leq \lfloor\sqrt{\phi(r)}log(n)\rfloor$

$$(X + a)^n = X^n + a\ mod(X^r - 1, n)$$

1. La première étape : déterminer si n est une puissance.
   On va donc tester pour chaque i s'il existe un $a_i \in N, a_i \geq 2$ tel que $n = a^i$.
   Cela équivaut à $i = \frac{ln(n)}{ln(a)}$ donc $i \leq log(n)$;il nous faut donc tester $O(log(n))$ valeurs de i. Donc la complexité de cette étape est en $O(log(n))$.

2. La deuxième étape : trouver r tel que $o_r(n) > log(n)^2$.
   On teste successivement les valeurs de r.
   Pour chaque r, on teste si on a : $n^k \equiv 1(mod\ r)$ pour un certain $k \leq log(n)^2$.
   Pour un r fixé, on aura une complexité de $O(log(n)^2)$.
   Et comme on a montré, en lemme 1.3 , que $r = O(log(n)^5)$, alors cette étape a une complexité de $O(log(n)^7)$.

3. la troisième étape a une complexité $O(log(n)^6)$

4. La quatrième étape : on a une complexité de $O(r^{\frac{3}{2}}.log(n)^3) = O(log(n)^{\frac{21}{2}})$.
   Cette complexité domine les autres et elle est donc celle de l'algorithme.[1]

Références

[1]. MANINDRA AGRAWAL, NEERAJ KAYAL, AND NITIN SAXENA, PRIMES IS IN P : Annals of Mathematics Second Series, Volume 160, Numéro 2 pp. 781-793, 2004

[2]. Julien Élie, L'algorithme AKS ou Les nombres premiers sont de classe P

[3]. R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge Univ. Press, Cambridge, 1986.

[4]. Solution du forum AOPS : https ://artofproblemsolving.com/community/c7h1247514p6413470

[5]. M. Nair : On Chebyshev-type inequalities for primes : Amer Math Monthly, 1982