

Primes is in P
Manindra Agrawal, Neeraj Kayal and Nitin Saxena

Nicolas Gast

15 février 2005

Plan

Introduction

Contexte

Preliminaires

L'algorithme

Détails

Correction : n premier $\Rightarrow$ PRIME

Correction : PRIME $\Rightarrow n$ premier

Complexité

Introduction

Introduction

Contexte

Preliminaires

L'algorithme

Détails

Correction : n premier $\Rightarrow$ PRIME

Correction : PRIME $\Rightarrow n$ premier

Complexité

Contexte

Test de primalités :

1. En $O(\sqrt{n})$
2. Problème co-NP, NP (1975)
3. Bons algo probabilistes

Ici

$O(\log(n)^{10.5})$

Contexte

Test de primalités :

1. En $O(\sqrt{n})$
2. Problème co-NP, NP (1975)
3. Bons algo probabilistes

Ici

$O(\log(n)^{10.5})$



Idée

- ▶ $a \in \mathbb{Z}$
- ▶ $n \in \mathbb{N}, n \geq 2, \text{GCD}(a, n) = 1$

n est premier si et seulement si

$$(X + a)^n = X^n + a \pmod{n} \quad (2.1)$$

Démonstration.

Le coefficient de X^i ($0 < i < n$) de $(X + a)^n$ est $c = \binom{n}{i} a^{n-i}$

- ▶ Si n est premier : $c = 0$
- ▶ Si $q^k \parallel n$, $q^k \nmid \binom{n}{q}$, or $\text{GCD}(n, a) = 1$ donc $\binom{n}{q} \neq 0$





Idée

- ▶ $a \in \mathbb{Z}$
- ▶ $n \in \mathbb{N}, n \geq 2, \text{GCD}(a, n) = 1$

n est premier si et seulement si

$$(X + a)^n = X^n + a \pmod{n} \quad (2.1)$$

Démonstration.

Le coefficient de X^i ($0 < i < n$) de $(X + a)^n$ est $c = \binom{n}{i} a^{n-i}$

- ▶ Si n est premier : $c = 0$
- ▶ Si $q^k \parallel n$, $q^k \nmid \binom{n}{q}$, or $\text{GCD}(n, a) = 1$ donc $\binom{n}{q} \neq 0$





Préliminaire

$o_r(a)$ (Ordre d'un modulo r)

Plus petit entier k tel que $a^k = 1(\text{mod } r)$

$\phi(r)$ (indicateur d'Euler)

nombre d'entier $\leq r$ premiers avec r

$LCM(m)$

Def : $LCM(m) = \text{ppcm des } m \text{ premiers entier}$

Theorem

$$LCM(m) \geq 2^m \quad (3.1)$$

Préliminaire

$o_r(a)$ (*Ordre d'un modulo r*)

Plus petit entier k tel que $a^k = 1(\text{mod } r)$

$\phi(r)$ (*indicateur d'Euler*)

nombre d'entier $\leq r$ premiers avec r

$LCM(m)$

Def : $LCM(m) = \text{ppcm des } m \text{ premiers entier}$

Theorem

$$LCM(m) \geq 2^m \quad (3.1)$$

Préliminaire

$o_r(a)$ (Ordre d'un modulo r)

Plus petit entier k tel que $a^k = 1(\text{mod } r)$

$\phi(r)$ (indicateur d'Euler)

nombre d'entier $\leq r$ premiers avec r

$\text{LCM}(m)$

Def : $\text{LCM}(m) = \text{ppcm}$ des m premiers entier

Theorem

$$\text{LCM}(m) \geq 2^m \quad (3.1)$$

L'algorithme

Introduction

Contexte

Preliminaires

L'algorithme

Détails

Correction : n premier $\Rightarrow$ PRIME

Correction : PRIME $\Rightarrow n$ premier

Complexité

L'algorithme

Prime(n)

1. **if** ($n = a^b$, $b > 1$) **output** COMPOSITE
2. Trouver le plus petit r tel que $o_r(n) > 4 \log^2 n$.
3. **If** $\exists a \leq r$ tel que $1 < \gcd(a, n)$, **output** COMPOSITE
4. **If** $n \leq r$ **output** PRIME
5. **For** $a = 1$ **to** $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$ **do**
 if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, **output** COMPOSITE
6. **Output** PRIME

Analyse de l'algorithme

1. Si n est premier, l'algorithme retourne PRIME
2. PRIME $\Rightarrow n$ premier
 - 2.1 Existence d'un $r \leq \lceil 16 \log^5 n \rceil$
 - 2.2 Définition d'un groupe, étude de sa cardinalité : et contradictions
3. Complexité
 - 3.1 Basique
 - 3.2 Améliorations

Analyse de l'algorithme

1. Si n est premier, l'algorithme retourne PRIME
2. PRIME $\Rightarrow n$ premier
 - 2.1 Existence d'un $r \leq \lceil 16 \log^5 n \rceil$
 - 2.2 Définition d'un groupe, étude de sa cardinalité : et contradictions
3. Complexité
 - 3.1 Basique
 - 3.2 Améliorations

Analyse de l'algorithme

1. Si n est premier, l'algorithme retourne PRIME
2. PRIME $\Rightarrow n$ premier
 - 2.1 Existence d'un $r \leq \lceil 16 \log^5 n \rceil$
 - 2.2 Définition d'un groupe, étude de sa cardinalité : et contradictions
3. Complexité
 - 3.1 Basique
 - 3.2 Améliorations

*Si n est premier, on retourne **PRIME***

Les lignes à étudier :

Ligne 1

if ($n = a^b$, $b > 1$) **output** COMPOSITE

Ligne 3

if $\exists a \leq r$ telque $1 < \gcd(a, n)$, **output** COMPOSITE

Ligne 5

For $a = 1$ to $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$ do
if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, **output** COMPOSITE

*Si n est premier, on retourne **PRIME***

Les lignes à étudier :

Ligne 1

if ($n = a^b$, $b > 1$) **output** COMPOSITE

Ligne 3

if $\exists a \leq r$ telque $1 < \gcd(a, n)$, **output** COMPOSITE

Ligne 5

For $a = 1$ to $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$ do
if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, **output** COMPOSITE

*Si n est premier, on retourne **PRIME***

Les lignes à étudier :

Ligne 1

if ($n = a^b$, $b > 1$) **output** COMPOSITE

Ligne 3

if $\exists a \leq r$ telque $1 < \gcd(a, n)$, **output** COMPOSITE

Ligne 5

For $a = 1$ to $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$ do
if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, **output** COMPOSITE

*Si n est premier, on retourne **PRIME***

Les lignes à étudier :

Ligne 1

if ($n = a^b$, $b > 1$) **output** COMPOSITE

Ligne 3

if $\exists a \leq r$ telque $1 < \gcd(a, n)$, **output** COMPOSITE

Ligne 5

For $a = 1$ to $\lfloor 2\sqrt{\phi(r)} \log n \rfloor$ do
if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, **output** COMPOSITE

Existence d'un $r \leq \lceil 16 \log^5 n \rceil$

Lemma

Il existe un $r \leq \lceil 16 \log^5 n \rceil$ tel que $o_r(n) > 4 \log^2 n$

Démonstration.

soit $r_1, r-2, r_t$ les nombres tels que $o_{r_i} < 4 \log^2 n$. Chaque r_i divise le produit

$$\prod_{i=1}^{\lceil 4 \log^2 n \rceil} (n^{r_i} - 1) < n^{16 \log^4 n} \leq 2^{16 \log^5 n}$$

Par le lemme 3.1 (LCM), on a donc un des $r_i \leq \lceil 16 \log^5 n \rceil$



Existence d'un $r \leq \lceil 16 \log^5 n \rceil$

Lemma

Il existe un $r \leq \lceil 16 \log^5 n \rceil$ tel que $o_r(n) > 4 \log^2 n$

Démonstration.

soit $r_1, r-2, r_t$ les nombres tels que $o_{r_i} < 4 \log^2 n$. Chaque r_i divise le produit

$$\prod_{i=1}^{\lceil 4 \log^2 n \rceil} (n^{r_i} - 1) < n^{16 \log^4 n} \leq 2^{16 \log^5 n}$$

Par le lemme 3.1 (LCM), on a donc un des $r_i \leq \lceil 16 \log^5 n \rceil$



Définition de G

- ▶ Soit p un diviseur de n
- ▶ Soit $I = \{n^i \cdot p^j \mid i, j \geq 0\}$

Définition : G

- ▶ G est l'ensemble des restes de I modulo r
- ▶ G est un sous-groupe de $\mathbb{Z}_r^*$ car $\gcd(n, r) = 1$
- ▶ G est engendré par n et p
- ▶ On pose $t = |G|$, $t \geq o_r(n) > 4 \log^2 n$

Définition de G

- ▶ Soit p un diviseur de n
- ▶ Soit $I = \{n^i \cdot p^j \mid i, j \geq 0\}$

Définition : G

- ▶ G est l'ensemble des restes de I modulo r
- ▶ G est un sous-groupe de $\mathbb{Z}_r^*$ car $\gcd(n, r) = 1$
- ▶ G est engendré par n et p
- ▶ On pose $t = |G|$, $t \geq o_r(n) > 4 \log^2 n$

Définition de $\mathcal{G}$

Définition

Soit $h(X)$ un facteur irréductible de $Q_r(X)$ dans F_p , le $r^{\text{ième}}$ polynôme cyclotomique. Il a degré $o_r(p)$

$\mathcal{G}$

$\mathcal{G}$ est l'ensemble des polynôme de P dont le reste modulo $h(X)$ et p est non nul.

$\mathcal{G}$ est généré par $X + 1, X + 2, \dots, X + l$ dans $F_p[X]/(h(X))$

Définition de $\mathcal{G}$

Définition

Soit $h(X)$ un facteur irréductible de $Q_r(X)$ dans F_p , le $r^{\text{ième}}$ polynôme cyclotomique. Il a degré $o_r(p)$

$\mathcal{G}$

$\mathcal{G}$ est l'ensemble des polynôme de P dont le reste modulo $h(X)$ et p est non nul.

$\mathcal{G}$ est généré par $X + 1, X + 2, \dots, X + l$ dans $F_p[X]/(h(X))$

Étude de la taille de $\mathcal{G}$

Lemma

$$|\mathcal{G}| \geq \binom{t+l-2}{t-1} \quad (4.7)$$

Lemma

Si n n'est pas une puissance de p :

$$|\mathcal{G}| < \frac{1}{2} n^{2\sqrt{t}} \quad (4.8)$$

Étude de la taille de $\mathcal{G}$

Lemma

$$|\mathcal{G}| \geq \binom{t+l-2}{t-1} \quad (4.7)$$

Lemma

Si n n'est pas une puissance de p :

$$|\mathcal{G}| < \frac{1}{2} n^{2\sqrt{t}} \quad (4.8)$$

Étude de la taille de $\mathcal{G}$

La contradiction

- ▶ D'après le lemme 4.7, en prenant $t = |G|$ et $l = \lceil 2\sqrt{\phi(r)} \log n \rceil$:

$$\begin{aligned}
 |\mathcal{G}| &\geq \binom{t+l-2}{t-1} \\
 &\geq \dots \\
 &\geq \frac{1}{2} n^{2\sqrt{t}}
 \end{aligned}$$

- ▶ Or d'après le lemme 4.8 : Si n n'est pas une puissance de p : $|\mathcal{G}| < \frac{1}{2} n^{2\sqrt{t}}$
- ▶ donc n est une puissance de p
- ▶ donc $n = p$

Étude de la complexité

Analyse

- | | |
|---|--|
| 1. if ($n = a^b$, $b > 1$) ... | 1. $O(\log^3(n))$ |
| 2. Trouver r ,
$o_r(n) > 4 \log^2 n$... | 2. recherche "exhaustive" :
$O(\log^7(n))$ |
| 3. If $\exists a \leq r$ tq $\gcd(a, n)$... | 3. $O(\log^6)$ |
| 4. If $n \leq r$... | 4. $O(\log n)$ |
| 5. For $a = 1$ to
$\lfloor 2\sqrt{\phi(r)} \log n \rfloor$
if $((X + a)^n \neq$
$X^n + a(\bmod X^r - 1, n))$ | 5. $\lfloor 2\sqrt{\phi(r)} \log n \rfloor \cdot \log^2 n =$
$O(\log^{10.5} n)$ |
- D'où : $O(\log^{10.5} n)$**

Conclusion

- ▶ Un algorithme polynomial pour la primalité
- ▶ Moins performant en pratique
- ▶ Utile pour les utilisations critiques
- ▶ Améliorations :
 - ▶ Lemme sur la taille de r : $O(\log^{7.5} n)$
 - ▶ Conjecture : si r est premier ne divisant pas n , alors $(X + 1)^n = X^n \pmod{X^r - 1, n}$ ssi n est premier ou $n^2 = 1 \pmod{r}$

Conclusion

- ▶ Un algorithme polynomial pour la primalité
- ▶ Moins performant en pratique
- ▶ Utile pour les utilisations critiques
- ▶ Améliorations :
 - ▶ Lemme sur la taille de r : $O(\log^{7.5} n)$
 - ▶ Conjecture : si r est premier ne divisant pas n , alors $(X + 1)^n = X^n \pmod{X^r - 1, n}$ ssi n est premier ou $n^2 = 1 \pmod{r}$

Conclusion

- ▶ Un algorithme polynomial pour la primalité
- ▶ Moins performant en pratique
- ▶ Utile pour les utilisations critiques
- ▶ Améliorations :
 - ▶ Lemme sur la taille de r : $O(\log^{7.5} n)$
 - ▶ Conjecture : si r est premier ne divisant pas n , alors $(X + 1)^n = X^n \pmod{X^r - 1, n}$ ssi n est premier ou $n^2 = 1 \pmod{r}$

Conclusion

- ▶ Un algorithme polynomial pour la primalité
- ▶ Moins performant en pratique
- ▶ Utile pour les utilisations critiques
- ▶ Améliorations :
 - ▶ Lemme sur la taille de r : $O(\log^{7.5} n)$
 - ▶ Conjecture : si r est premier ne divisant pas n , alors $(X + 1)^n = X^n \pmod{X^r - 1, n}$ ssi n est premier ou $n^2 = 1 \pmod{r}$