COMPLEX
Cours 8 - Algorithmes algébriques probabilistes

Damien Vergnaud

Sorbonne Université – CNRS

Table des matières

Disquisitiones Arithmeticae – C. F. Gauss (1801)

Article 329

Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resolvendi, ad gravissima ac utilissima totius arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupavisse, tam notum est, ut de hac re copiose loqui superfluum foret. . . . [P]raetereaque scientiae dignitas requirere videtur, ut omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur.

Disquisitiones Arithmeticae – C. F. Gauss (1801)

Article 329

Le problème de la distinction entre les nombres premiers et les nombres composés et de la factorisation de ces derniers en leurs facteurs premiers est connu pour être l'un des plus importants et des plus utiles en arithmétique. Il a fait appel à l'industrie et à la sagesse des géomètres anciens et modernes à un point tel qu'il serait superflu de discuter longuement du problème. . . . En outre, la dignité de la science elle-même semble exiger que tous les moyens possibles soient explorés pour la solution d'un problème aussi élégant et aussi célèbre.

Primalité

Primalité

- Entrée : $n \geq 2$ un entier
- Sortie : vrai si n est premier et faux sinon

Notations

- $\mathbb{P}$ = ensemble des nombres premiers
- $\mathbb{N} \setminus (\mathbb{P} \cup \{0, 1\})$ = ensemble des nombres composés

Composition

- Entrée : $n \geq 2$ un entier
- Sortie : vrai si n composé et faux sinon

Primalité

Primalité

- Entrée : $n \geq 2$ un entier
- Sortie : vrai si n est premier et faux sinon

Notations

- $\mathbb{P}$ = ensemble des nombres premiers
- $\mathbb{N} \setminus (\mathbb{P} \cup \{0, 1\})$ = ensemble des nombres composés

Composition

- Entrée : $n \geq 2$ un entier
- Sortie : vrai si n composé et faux sinon

Algorithme naïf

Entrée: $n \in \mathbb{N}$
Sortie: Composé ou Premier

pour i de 2 à $n-1$ **faire**
  si $i \mid n$ **alors**
    retourner Composé
  fin si
fin pour
retourner Premier

Complexité

Nombres de divisions :

Algorithme naïf

Entrée: $n \in \mathbb{N}$
Sortie: $\textsc{Composé}$ ou $\textsc{Premier}$

pour i de 2 à $n-1$ **faire**
  si $i \mid n$ **alors**
    retourner $\textsc{Composé}$
  fin si
fin pour
retourner $\textsc{Premier}$

Complexité

Nombres de divisions :

Algorithme naïf

Entrée: $n \in \mathbb{N}$
Sortie: $\textsc{Composé}$ ou $\textsc{Premier}$

```
pour i de 2 à n − 1 faire
    si i | n alors
        retourner COMPOSÉ
    fin si
fin pour
retourner PREMIER
```

Complexité

Nombres de divisions : $O(n)$

Représentation des entiers et complexité

- Le nombre d'atomes de l'univers $n \simeq 10^{80}$
- Écrire n demande **seulement** 81 chiffres décimaux (266 chiffres binaires)
- Un entier n se représente avec $t = \lceil \log(n) \rceil$ chiffres binaires
- L'algorithme naïf a donc une complexité de

$$O(n) = O(2^t) \text{ divisions}$$

Il a une complexité **exponentielle**

- PRIMALITÉ $\in \mathcal{EXP}$ (et COMPOSITION $\in \mathcal{EXP}$)

Représentation des entiers et complexité

- Le nombre d'atomes de l'univers $n \simeq 10^{80}$
- Écrire n demande **seulement** 81 chiffres décimaux (266 chiffres binaires)

- Un entier n se représente avec $t = \lceil \log(n) \rceil$ chiffres binaires
- L'algorithme naïf a donc une complexité de

$$O(n) = O(2^t) \text{ divisions}$$

Il a une complexité **exponentielle**

- PRIMALITÉ $\in \mathcal{EXP}$ (et COMPOSITION $\in \mathcal{EXP}$)

Représentation des entiers et complexité

- Le nombre d'atomes de l'univers $n \simeq 10^{80}$
- Écrire n demande **seulement** 81 chiffres décimaux (266 chiffres binaires)

- Un entier n se représente avec $t = \lceil \log(n) \rceil$ chiffres binaires
- L'algorithme naïf a donc une complexité de

$$O(n) = O(2^t) \text{ divisions}$$

Il a une complexité **exponentielle**

- $\textsc{Primalité} \in \mathcal{EXP}$ (et $\textsc{Composition} \in \mathcal{EXP}$)

Algorithme (un peu) moins naïf

Entrée: $n \in \mathbb{N}$
Sortie: Composé ou Premier

pour i de 2 à $\lfloor \sqrt{n} \rfloor$ **faire**
  si $i \mid n$ **alors**
    retourner Composé
  fin si
fin pour
retourner Premier

Complexité

Nombres de divisions :

Algorithme (un peu) moins naïf

Entrée: $n \in \mathbb{N}$
Sortie: $\textsc{Composé}$ ou $\textsc{Premier}$

> **pour** i de 2 à $\lfloor \sqrt{n} \rfloor$ **faire**
>   **si** $i \mid n$ **alors**
>   **retourner** $\textsc{Composé}$
>   **fin si**
> **fin pour**
> **retourner** $\textsc{Premier}$

Complexité

Nombres de divisions :

Algorithme (un peu) moins naïf

Entrée: $n \in \mathbb{N}$
Sortie: COMPOSÉ ou PREMIER

pour i de 2 à $\lfloor \sqrt{n} \rfloor$ **faire**
  si $i \mid n$ **alors**
    retourner COMPOSÉ
  fin si
fin pour
retourner PREMIER

Complexité

Nombres de divisions : $O(\sqrt{n}) = O(2^{t/2}) = O(\sqrt{2^t})$

Algorithme (un peu) moins naïf

Entrée: $n \in \mathbb{N}$
Sortie: Composé ou Premier

pour i de 2 à $\lfloor \sqrt{n} \rfloor$ **faire**
  si $i \mid n$ **alors**
    retourner Composé
  fin si
fin pour
retourner Premier

Complexité

Nombres de divisions : $O(\sqrt{n}) = O(2^{t/2}) = O(\sqrt{2^t})$

- Primalité $\in \mathcal{EXP}$ (et Composition $\in \mathcal{EXP}$)

Théorème des nombres premiers

Euclide (*circa* - 300)

Il existe une infinité de nombres premiers

Fonction $\pi(x)$

$$\pi(x) = \#\{n \leq x | n \in \mathbb{P}\} = \#(\mathbb{P} \cap [2, x])$$

Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

Théorème des nombres premiers

Euclide (*circa* - 300)

Il existe une infinité de nombres premiers

Fonction $\pi(x)$

$$\pi(x) = \#\{n \leq x | n \in \mathbb{P}\} = \#(\mathbb{P} \cap [2, x])$$

Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

Théorème des nombres premiers

Euclide (*circa* - 300)

Il existe une infinité de nombres premiers

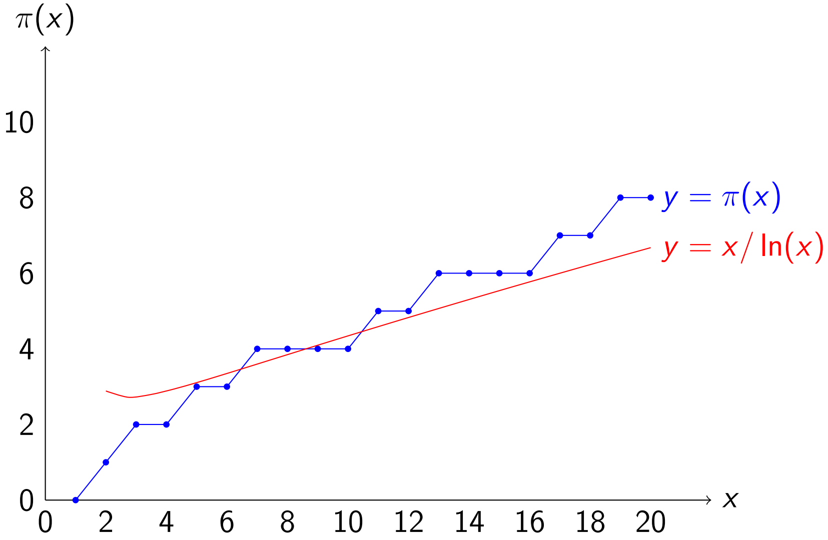
Fonction $\pi(x)$

$$\pi(x) = \#\{n \leq x | n \in \mathbb{P}\} = \#(\mathbb{P} \cap [2, x])$$

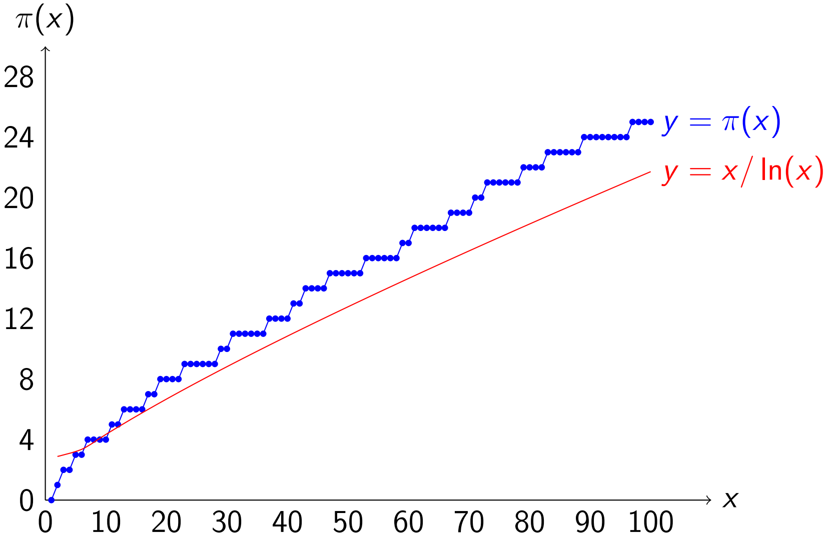
Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

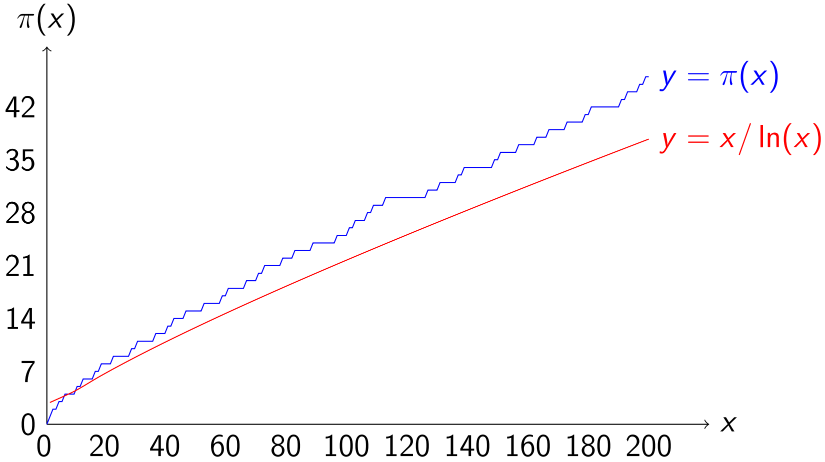
Théorème des nombres premiers



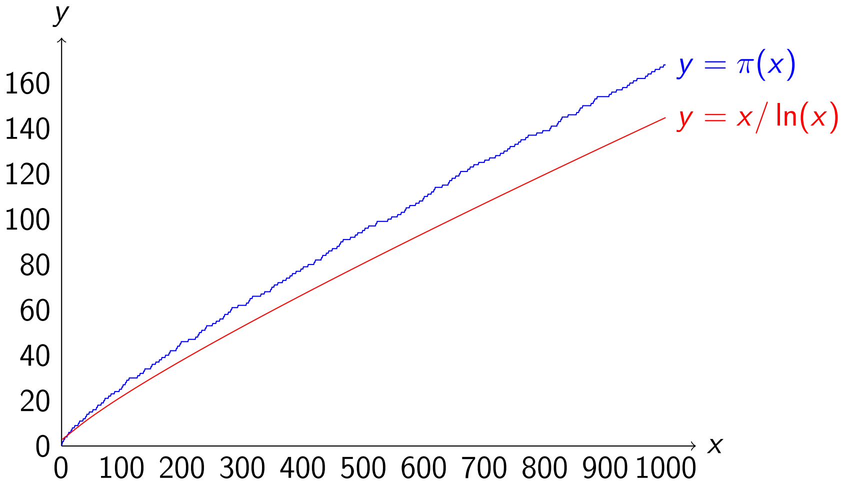
Théorème des nombres premiers



Théorème des nombres premiers



Théorème des nombres premiers



Théorème des nombres premiers

Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

- p_n = le n-ième nombre premier $p_n \rightsquigarrow p_n \sim n \ln(n)$
- Pour $x \geq 55$
$$. \frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}$$
- Pour n tiré uniformément aléatoirement dans $\{1, \ldots, N\}$:
$$\Pr(n \in \mathbb{P}) \simeq \frac{1}{\ln(N)}$$

Théorème des nombres premiers

Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

- p_n = le n-ième nombre premier $p_n \rightsquigarrow p_n \sim n\ln(n)$
- Pour $x \geq 55$

$$.\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}$$

- Pour n tiré uniformément aléatoirement dans $\{1, \ldots, N\}$:

$$\Pr(n \in \mathbb{P}) \simeq \frac{1}{\ln(N)}$$

Théorème des nombres premiers

Théorème des nombres premiers
J. Hadamard et Ch. de La Vallée Poussin (1896)

$$\pi(x) \sim \frac{x}{\ln(x)} \qquad (x \to +\infty)$$

- p_n = le n-ième nombre premier $p_n \rightsquigarrow p_n \sim n \ln(n)$
- Pour $x \geq 55$
$$.\frac{x}{\ln x + 2} < \pi(x) < \frac{x}{\ln x - 4}$$
- Pour n tiré uniformément aléatoirement dans $\{1, \ldots, N\}$:

$$\Pr(n \in \mathbb{P}) \simeq \frac{1}{\ln(N)}$$

Primalité $\in$ co$-\mathcal{NP}$

- Composition $\in \mathcal{NP}$
- n composé $\rightsquigarrow n = d \cdot m$ avec $d, n, m \in \mathbb{N}$ et $d \notin \{1, n\}$

Entrée: $n \in \mathbb{N}$; $d \in \mathbb{N}$
Sortie: Composé ou Témoin invalide

si $d \neq 1 \wedge d \neq n \wedge d \mid n$ **alors**
  retourner Composé
sinon
  retourner Témoin invalide
fin si

PRIMALITÉ $\in$ co$-\mathcal{NP}$

- COMPOSITION $\in \mathcal{NP}$
- n composé $\rightsquigarrow n = d \cdot m$ avec $d, n, m \in \mathbb{N}$ et $d \notin \{1, n\}$

Entrée: $n \in \mathbb{N}$; $d \in \mathbb{N}$
Sortie: COMPOSÉ ou TÉMOIN INVALIDE

si $d \neq 1 \wedge d \neq n \wedge d \mid n$ **alors**
  retourner COMPOSÉ
sinon
  retourner TÉMOIN INVALIDE
fin si

PRIMALITÉ $\in \mathcal{NP}$

- semble plus difficile !
- qu'un entier ne soit pas diviseur, ne prouve rien . . .
- il faut montrer l'existence d'un « objet »
  - qui existe si et seulement n est premier
  - de « petite » taille (c.-à-d. polynomiale en $\log(n)$)
  - dont les propriétés se vérifient efficacement (c.-à-d. en temps polynomial en $\log(n)$)

Primalité $\in \mathcal{NP}$

- semble plus difficile !
- qu'un entier ne soit pas diviseur, ne prouve rien ...

- il faut montrer l'existence d'un « objet »
  - qui existe si et seulement n est premier
  - de « petite » taille (c.-à-d. polynomiale en $\log(n)$)
  - dont les propriétés se vérifient efficacement (c.-à-d. en temps polynomial en $\log(n)$)

PRIMALITÉ $\in \mathcal{NP}$

- semble plus difficile !
- qu'un entier ne soit pas diviseur, ne prouve rien ...

- il faut montrer l'existence d'un « objet »
  - qui existe si et seulement n est premier
  - de « petite » taille (c.-à-d. polynomiale en $\log(n)$)
  - dont les propriétés se vérifient efficacement (c.-à-d. en temps polynomial en $\log(n)$)

Proposition

Un entier $n \geq 2$ est premier si et seulement $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe cyclique d'ordre $n - 1$

PRIMALITÉ $\in \mathcal{NP}$

- semble plus difficile !
- qu'un entier ne soit pas diviseur, ne prouve rien ...

- il faut montrer l'existence d'un « objet »
  - qui existe si et seulement n est premier
  - de « petite » taille (c.-à-d. polynomiale en $\log(n)$)
  - dont les propriétés se vérifient efficacement (c.-à-d. en temps polynomial en $\log(n)$)

Théorème de Lucas

Un entier $n \geq 2$ est premier si et seulement s'il existe un entier $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{(n-1)/q} \not\equiv 1 \bmod n$ pour tout diviseur premier q de $n - 1$.

PRIMALITÉ $\in \mathcal{NP}$ – Exemple

- $n = 71\,;\ n - 1 = 70 = 2 \times 5 \times 7$
- $a = 17$

$$\begin{cases} 17^{35} & \equiv & 70 \bmod 71 \neq 1 \bmod 71 \\ 17^{14} & \equiv & 25 \bmod 71 \neq 1 \bmod 71 \\ 17^{10} & \equiv & 1 \bmod 71 \end{cases}$$

- $a = 11$

$$\begin{cases} 11^{35} & \equiv & 70 \bmod 71 \neq 1 \bmod 71 \\ 11^{14} & \equiv & 54 \bmod 71 \neq 1 \bmod 71 \\ 11^{10} & \equiv & 32 \bmod 71 \neq 1 \bmod 71 \end{cases}$$

et $11^{70} \equiv 1 \bmod 71 \rightsquigarrow 71$ est premier !

PRIMALITÉ $\in \mathcal{NP}$ – Exemple

- $n = 71\,;\ n - 1 = 70 = 2 \times 5 \times 7$
- $a = 17$

$$\begin{cases} 17^{35} & \equiv & 70 \bmod 71 \neq 1 \bmod 71 \\ 17^{14} & \equiv & 25 \bmod 71 \neq 1 \bmod 71 \\ 17^{10} & \equiv & 1 \bmod 71 \end{cases}$$

- $a = 11$

$$\begin{cases} 11^{35} & \equiv & 70 \bmod 71 \neq 1 \bmod 71 \\ 11^{14} & \equiv & 54 \bmod 71 \neq 1 \bmod 71 \\ 11^{10} & \equiv & 32 \bmod 71 \neq 1 \bmod 71 \end{cases}$$

et $11^{70} \equiv 1 \bmod 71 \rightsquigarrow 71$ est premier !

Exponentiation rapide (variante récursive)

$$a^x \bmod n = \begin{cases} 1 & \text{si } x = 0 \\ (a^{x/2})^2 \bmod n & \text{si } x > 0 \text{ est pair} \\ a \cdot (a^{(x-1)/2})^2 \bmod n & \text{si } x > 0 \text{ est impair} \end{cases}$$

$\rightsquigarrow$ algorithme récursif !

Exponentiation rapide (variante récursive)

Entrée: $(n, a, x) \in \mathbb{N}^3$ avec $n \geq 2$ et $a \geq 1$
Sortie: $a^x \bmod n$

si $x = 0$ **alors**
  retourner 1
sinon si $x \bmod 2 = 0$ **alors**
  $b \leftarrow \text{Exponentiation}(n, a, x/2)$
  retourner $b^2 \bmod n$
sinon
  $b \leftarrow \text{Exponentiation}(n, a, (x-1)/2)$
  retourner $a \cdot b^2 \bmod n$
fin si

Exponentiation rapide (variante itérative)

$$x = \sum_{i=0}^{\ell-1} x_i 2^i \in \mathbb{N} \text{ avec } x_i \in \{0,1\} \text{ pour } i \in \{0,\dots,\ell-1\},$$

$$\begin{aligned} a^x = \prod_{i=0}^{\ell-1} a^{x_i 2^i} &= a^{x_0} \left(a^{x_1}\right)^2 \left(a^{x_2}\right)^4 \left(a^{x_3}\right)^8 \dots \left(a^{x_{\ell-1}}\right)^{2^{\ell-1}} \\ &= a^{x_0} \left(a^{x_1} \left(a^{x_2} \left(a^{x_3} \dots \left(a^{x_{\ell-1}} \dots \right)^2 \right)^2 \right)^2 \right)^2 . \end{aligned}$$

$\rightsquigarrow$ algorithme itératif !

Exponentiation rapide (variante itérative)

Entrée: $(n, a, x) \in \mathbb{N}^3$ avec $n \geq 2$ et $a \geq 1$ $\qquad \triangleright\ x = \sum_{i=0}^{\ell-1} x_i 2^i$

Sortie: $a^x \bmod n$

$h \leftarrow 1$
pour i de $\ell - 1$ à 0 **faire**
  $h \leftarrow h^2 \bmod n$ $\qquad \triangleright$ l'indice i varie en décroissant
  si $x_i = 1$ **alors**
    $h \leftarrow h \cdot a \bmod n$
  fin si
fin pour
retourner h

Primalité $\in \mathcal{NP}$

Théorème de Lucas

Un entier $n \geq 2$ est premier si et seulement s'il existe un entier $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{(n-1)/q} \not\equiv 1 \bmod n$ pour tout diviseur premier q de $n-1$.

Primalité de $n \rightsquigarrow (a, q_1, \ldots, q_t) \in \mathbb{N}$

- $a^{n-1} \equiv 1 \bmod n$ $\triangleright$ exponentiation rapide
- $n - 1 = q_1 \ldots q_t$ $\triangleright$ $t-1$ multiplications
- $a^{(n-1)/q_i} \not\equiv 1 \bmod n$ pour $i \in \{1, \ldots, t\}$ $\triangleright$ t exponentiations rapides
- q_i premiers $\triangleright$ certificats récursifs ...

Certificats de Pratt

1975 – V. Pratt (analyse détaillée en TD)

Petit théorème de Fermat

Petit théorème de Fermat

Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv 1 \bmod p$.

- **Contraposée :** pour $n \geq 2$ entier
  - $\exists a \in \{2, n-1\}, a^{n-1} \not\equiv 1 \bmod n \rightsquigarrow$ n composé
  - $\exists a \in \{2, n-1\}, a^{n-1} \equiv 1 \bmod n \rightsquigarrow n$ **?**

Test de Fermat

Entrée: $n \in \mathbb{N}$ impair ; $a \in \mathbb{N}$
Sortie: COMPOSÉ ou PREMIER POSSIBLE

$b \leftarrow a^{n-1} \bmod n$ ▷ par exponentiation rapide
si $b \neq 1$ **alors**
retourner COMPOSÉ
fin si
retourner PREMIER POSSIBLE

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

Test de Fermat

Entrée: $n \in \mathbb{N}$ impair ; $a \in \mathbb{N}$
Sortie: COMPOSÉ ou PREMIER POSSIBLE

$b \leftarrow a^{n-1} \bmod n$ ▷ par exponentiation rapide
si $b \neq 1$ **alors**
retourner COMPOSÉ
fin si
retourner PREMIER POSSIBLE

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$?

Test de Fermat

Entrée: $n \in \mathbb{N}$ impair ; $a \in \mathbb{N}$
Sortie: COMPOSÉ ou PREMIER POSSIBLE

$b \leftarrow a^{n-1} \bmod n$ $\triangleright$ par exponentiation rapide
si $b \neq 1$ **alors**
  retourner COMPOSÉ
fin si
retourner PREMIER POSSIBLE

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

Nombres pseudo-premiers de Fermat

Soit $a \in \mathbb{N}$, $a \geq 2$. Un entier composé n est un nombre pseudo-premier de Fermat en base a si $a^{n-1} \equiv 1 \bmod n$

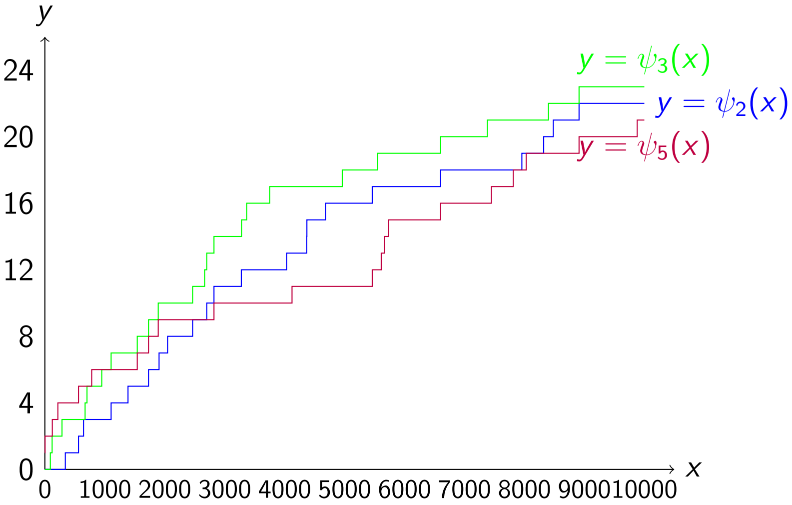
- **Base 2** : 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, ...
- **Base 3** : 91, 121, 286, 671, 703, 949, 1105, 1541, 1729, 1891, 2465, 2665, 2701, 2821, 3281, 3367, 3751, 4961, 5551, 6601, 7381, 8401, 8911, ...
- **Base 5** : 4, 124, 217, 561, 781, 1541, 1729, 1891, 2821, 4123, 5461, 5611, 5662, 5731, 6601, 7449, 7813, 8029, 8911, ...

Nombres pseudo-premiers de Fermat

Soit $a \in \mathbb{N}$, $a \geq 2$. Un entier composé n est un nombre pseudo-premier de Fermat en base a si $a^{n-1} \equiv 1 \bmod n$

- **Base 2** : 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, ...
- **Base 3** : 91, 121, 286, 671, 703, 949, 1105, 1541, 1729, 1891, 2465, 2665, 2701, 2821, 3281, 3367, 3751, 4961, 5551, 6601, 7381, 8401, 8911, ...
- **Base 5** : 4, 124, 217, 561, 781, 1541, 1729, 1891, 2821, 4123, 5461, 5611, 5662, 5731, 6601, 7449, 7813, 8029, 8911, ...

Nombres pseudo-premiers de Fermat



Nombres pseudo-premiers de Fermat

Théorème (Cipolla – 1904)

Soit $a \in \mathbb{N}$, $a \geq 2$. Il existe une infinité de nombres pseudo-premiers de Fermat en base a.

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

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

est pseudo-premier de Fermat en base a.

Nombres pseudo-premiers de Fermat

Théorème (Cipolla – 1904)

Soit $a \in \mathbb{N}$, $a \geq 2$. Il existe une infinité de nombres pseudo-premiers de Fermat en base a.

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

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

est pseudo-premier de Fermat en base a.

Nombres pseudo-premiers de Fermat

Théorème (Cipolla – 1904)

Soit $a \in \mathbb{N}$, $a \geq 2$. Il existe une infinité de nombres pseudo-premiers de Fermat en base a.

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

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

est pseudo-premier de Fermat en base a.

- 1 est racine de $X^p - 1$
- -1 est racine de $X^p + 1$

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow n \text{ composé}$$

- 2 divise $(n-1)$:

$$n - 1 = \frac{a^{2p} - a^2}{a^2 - 1} = \sum_{i=1}^{p-1} (a^2)^i \equiv (p-1) \cdot a \bmod 2 \equiv 0 \bmod 2$$

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow \textcolor{red}{n \text{ composé}}$$

- 2 divise $(n-1)$:

$$n - 1 = \frac{a^{2p} - a^2}{a^2 - 1} = \sum_{i=1}^{p-1} (a^2)^i \equiv (p-1) \cdot a \bmod 2 \equiv 0 \bmod 2$$

- p divise $(n-1)$:

$$\text{Fermat} \rightsquigarrow \left.\begin{array}{r} p \mid a^{2p} - a^2 \\ p \nmid a^2 - 1 \end{array}\right\} \rightsquigarrow p \mid \frac{a^{2p} - a}{a^2 - 1} = n - 1$$

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow n \text{ composé}$$

- $2p$ divise $(n - 1)$

$$(n - 1) = 2p \cdot \lambda$$

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow n \text{ composé}$$

- $2p$ divise $(n - 1)$

$$(n - 1) = 2p \cdot \lambda$$

- n divise $a^{2p} - 1$

$$a^{2p} \equiv 1 \bmod n$$

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow n \text{ composé}$$

- $2p$ divise $(n-1)$

$$(n-1) = 2p \cdot \lambda$$

- n divise $a^{2p} - 1$

$$a^{2p} \equiv 1 \bmod n$$

- $a^{n-1} \equiv 1 \bmod n$ $\qquad$ (car $a^{n-1} = a^{2p\cdot\lambda} = (a^{2p})^{\lambda} \equiv 1^{\lambda} \bmod n$)

Nombres pseudo-premiers de Fermat

Démonstration : Pour tout $p \in \mathbb{P}$ impair tel que $p \nmid (a^2 - 1)$,

$$n = \frac{a^{2p} - 1}{a^2 - 1} \quad \rightsquigarrow n \text{ composé}$$

- $2p$ divise $(n-1)$

$$(n-1) = 2p \cdot \lambda$$

- n divise $a^{2p} - 1$

$$a^{2p} \equiv 1 \bmod n$$

- $a^{n-1} \equiv 1 \bmod n$ $\qquad$ (car $a^{n-1} = a^{2p\cdot\lambda} = (a^{2p})^{\lambda} \equiv 1^{\lambda} \bmod n$)

□

Nombres pseudo-premiers de Fermat

- si le test de Fermat retourne PREMIER POSSIBLE, rien ne peut être décidé
- Les nombres pseudo-premiers de Fermat sont relativement rares

$$\psi_2(x) \leq x \cdot \exp\left(\frac{-\ln x \ln\ln\ln x}{2\ln\ln x}\right)$$

  (1980, C. Pomerance)
- Une idée naturelle est d'exécuter le test de Fermat sur plusieurs bases différentes ...

Nombres de Carmichael

- ... mais ça ne marche pas non plus !

Nombres de Carmichael

Un entier composé n est un nombre de Carmichael si pour tout entier a premier avec n, n est pseudo-premier de Fermat en base a (c.-à-d. $a^{n-1} \equiv 1 \bmod n$)

- **Exemples :** 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, ...

Critère de Korselt

Critère de Korselt

Un entier composé n est un nombre de Carmichael si et seulement si il possède les propriétés suivantes :

1. n est impair
2. n est sans facteur carré
3. pour tout nombre premier p qui divise n, $(p-1)$ divise $(n-1)$

Exemple :

$$561 = 3 \times 11 \times 17$$

et

$$560 = 2^4 \times 5 \times 7 = 2 \times 280 = 10 \times 56 = 16 \times 35$$

Nous verrons une démonstration de ce critère en TD

Nombres de Carmichael

- Les nombres de Carmichael sont relativement rares

$$C(x) \leq x \cdot \exp\left(\frac{-\ln x \ln\ln\ln x}{2\ln\ln x}\right)$$

(1980, C. Pomerance)

Théorème (W. R. Alford, A. Granville, C. Pomerance – 1994)

Il existe une infinité de nombres de Carmichael.

- si le test de Fermat retourne Premier Possible même sur plusieurs bases, rien ne peut être décidé !

Nombres pseudo-premiers forts

Critère d'Euler

Soit p un nombre premier impair. Pour tout entier a premier avec p,

$$a^{(p-1)/2} \bmod n \in \{1, p-1\}$$

Cette valeur vaut 1 si et seulement si a est un carré modulo p.

- Plus généralement, si x est solution de l'équation $X^2 = 1$ modulo un nombre premier p, alors $x = 1 \bmod p$ ou $x = -1 \bmod p$
- Attention, ce n'est pas vrai modulo un nombre composé !
  Exemple : L'équation $X^2 = 1$ a quatre solutions modulo 35 : $x = 1$, $x = 34 \equiv -1 \bmod 35$, $x = 6$ et $x = 29 \equiv -6 \bmod 35$.

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"] & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, bend left, dotted] & a^{2^t m} \arrow[r, bend left, dotted] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m}
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"] & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, dotted, bend left] & a^{2^t m} \arrow[r, dotted, bend left] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
 & & & & & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"] & & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, bend left, dotted] & a^{2^t m} \arrow[r, bend left, dotted] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
 & & & & \pm 1 & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"] \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, dotted, bend left] & a^{2^t m} \arrow[r, dotted, bend left] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
 & & & & 1 & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"'] & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, dotted, bend left] & a^{2^t m} \arrow[r, dotted, bend left] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
& & & \pm 1 & 1 & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"'] & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, dotted, bend left] & a^{2^t m} \arrow[r, dotted, bend left] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
 & \pm 1 & 1 & 1 & 1 & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

$$\boxed{p = 1 + 2^h m \in \mathbb{N}, \text{ avec } m \text{ impair}}$$

$$\begin{tikzcd}
a \arrow[d, bend right, "\text{puissance } m"] & & & & & \\
a^m \arrow[r, bend left, "\text{carré}"] & a^{2m} \arrow[r, bend left, "\text{carré}"] & a^{4m} \arrow[r, dotted, bend left] & a^{2^t m} \arrow[r, dotted, bend left] & a^{2^{h-1} m} \arrow[r, bend left, "\text{carré}"] & a^{2^h m} \\
\pm 1 & 1 & 1 & 1 & 1 & 1
\end{tikzcd}$$

Nombres pseudo-premiers forts

Soit $a \in \mathbb{N}$, $a \geq 2$. Un entier composé $n = 2^h m + 1$ (avec $h \geq 1$ et m impair) est un nombre pseudo-premier fort en base a si en notant :

$$b_0 = a^m \bmod n, \quad b_1 = b_0^2 \bmod n, \quad \ldots, \quad b_h = b_{h-1}^2 \bmod n$$

nous avons

- $b_h \equiv 1 \bmod n$
- si $b_0 \not\equiv 1 \bmod n$, il existe $i \in \{0, \ldots, h-1\}$ t.q. $b_i \equiv -1 \bmod n$.

- **Base 2 :** 2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, 52633, 65281, 74665, 80581, 85489, 88357, 90751, ...
- **Base 3 :** 121, 703, 1891, 3281, 8401, 8911, 10585, 12403, 16531, 18721, 19345, 23521, 31621, 44287, 47197, ...

Nombres pseudo-premiers forts

Soit $a \in \mathbb{N}$, $a \geq 2$. Un entier composé $n = 2^h m + 1$ (avec $h \geq 1$ et m impair) est un nombre pseudo-premier fort en base a si en notant :

$$b_0 = a^m \bmod n, \quad b_1 = b_0^2 \bmod n, \quad \ldots, \quad b_h = b_{h-1}^2 \bmod n$$

nous avons

- $b_h \equiv 1 \bmod n$
- si $b_0 \not\equiv 1 \bmod n$, il existe $i \in \{0, \ldots, h-1\}$ t.q. $b_i \equiv -1 \bmod n$.

- **Base 2 :** 2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, 52633, 65281, 74665, 80581, 85489, 88357, 90751, ...
- **Base 3 :** 121, 703, 1891, 3281, 8401, 8911, 10585, 12403, 16531, 18721, 19345, 23521, 31621, 44287, 47197, ...

Nombres pseudo-premiers forts

Entrée: $n = 1 + 2^h m \in \mathbb{N}$, avec m impair ; $a \in \mathbb{N}$
Sortie: Composé ou Premier Possible

```
b ← a^m mod n                              ▷ par exponentiation rapide
si b ≠ 1 et b ≠ n − 1 alors
    pour j de 1 à h − 1 faire
        si b ≠ n − 1 et b^2 mod n = 1 alors
            retourner Composé
        sinon si b = n − 1 alors
            retourner Premier Possible
        fin si
        b ← b^2 mod n
    fin pour
    si b ≠ n − 1 alors
        retourner Composé
    fin si
fin si
retourner Premier Possible
```

Nombres pseudo-premiers forts

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

- Les nombres pseudo-premiers forts sont relativement rares
- Il existe une infinité pour toute base a fixée
- Une idée naturelle est d'exécuter le test sur plusieurs bases différentes ...

Nombres pseudo-premiers forts

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

- Les nombres pseudo-premiers forts sont relativement rares
- Il existe une infinité pour toute base a fixée
- Une idée naturelle est d'exécuter le test sur plusieurs bases différentes . . .

Nombres pseudo-premiers forts

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

- Les nombres pseudo-premiers forts sont relativement rares
- Il existe une infinité pour toute base a fixée
- Une idée naturelle est d'exécuter le test sur plusieurs bases différentes ...

Nombres pseudo-premiers forts

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

- Les nombres pseudo-premiers forts sont relativement rares
- Il existe une infinité pour toute base a fixée
- Une idée naturelle est d'exécuter le test sur plusieurs bases différentes …

Nombres pseudo-premiers forts

Complexité

$$O(\log(a)\log(n) + \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER POSSIBLE $\rightsquigarrow$ **?**

- Les nombres pseudo-premiers forts sont relativement rares
- Il existe une infinité pour toute base a fixée
- Une idée naturelle est d'exécuter le test sur plusieurs bases différentes . . .

Nombres de Carmichael forts ?

- . . . et cette fois, ça marche !

- Il **n'existe pas** de « nombre de Carmichael fort »

Théorème de Rabin-Monier (1980)

Soit n un entier composé impair. Le nombre d'éléments a de $\{1, \ldots, n-1\}$ premiers avec n pour lequel n est pseudo-premier fort en base a est inférieur ou égal à $\varphi(n)/4$.

- Si n est un entier composé impair, la probabilité qu'un élément a tiré uniformément aléatoirement dans $\{1, \ldots, n-1\}$ soit tel que n est pseudo-premier fort en base a est :

$$\leq \frac{\varphi(n)/4}{n} \leq \frac{\varphi(n)/4}{\varphi(n)} = \frac{1}{4}$$

Nombres de Carmichael forts ?

- … et cette fois, ça marche !

- Il **n'existe pas** de « nombre de Carmichael fort »

Théorème de Rabin-Monier (1980)

Soit n un entier composé impair. Le nombre d'éléments a de $\{1, \dots, n-1\}$ premiers avec n pour lequel n est pseudo-premier fort en base a est inférieur ou égal à $\varphi(n)/4$.

- Si n est un entier composé impair, la probabilité qu'un élément a tiré uniformément aléatoirement dans $\{1, \dots, n-1\}$ soit tel que n est pseudo-premier fort en base a est :

$$\leq \frac{\varphi(n)/4}{n} \leq \frac{\varphi(n)/4}{\varphi(n)} = \frac{1}{4}$$

Test de Miller-Rabin

Entrée: $n = 1 + 2^h m \in \mathbb{N}$, avec m impair
Sortie: COMPOSÉ ou PREMIER

pour i de 1 à T **faire**

$a \longleftarrow (\mathbb{Z}/n\mathbb{Z})^*$

si NOMBRE_PSEUDO-PREMIER_FORT(n,a) = COMPOSÉ **alors**

retourner COMPOSÉ

fin si

fin pour

retourner PREMIER

Test de Miller-Rabin – PRIMALITÉ $\in \mathcal{BPP}$

Complexité

$$O(T \cdot \log(n)^3)$$

Validité

- COMPOSÉ $\rightsquigarrow$ toujours correct
- PREMIER $\rightsquigarrow \leq 4^{-T}$

Algorithme de type Monte-Carlo

Test de Miller-Rabin – Primalité $\in \mathcal{BPP}$

Complexité

$$O(T \cdot \log(n)^3)$$

Validité

- Composé $\rightsquigarrow$ toujours correct
- Premier $\rightsquigarrow \leq 4^{-T}$

Algorithme de type Monte-Carlo

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

  tant que VRAI **faire**
    $p \xleftarrow{} [2^{k-1}, 2^k]$
    si MILLER-RABIN(p,T) **alors**
      retourner p
    fin si
  fin tant que

Complexité

Complexité en moyenne $O(T \cdot k^4)$

Validité

Probabilité d'erreur $\rightsquigarrow \leq 4^{-T}$

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

  tant que VRAI **faire**

    $p \xleftarrow{} [2^{k-1}, 2^k]$

    si MILLER-RABIN(p,T) **alors**

      retourner p

    fin si

  fin tant que

Complexité

Complexité en moyenne $O(T \cdot k^4)$

Validité

Probabilité d'erreur $\rightsquigarrow \leq 4^{-T}$

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

tant que VRAI **faire**
  $p \xleftarrow{} [2^{k-1}, 2^k]$
  si Miller-Rabin(p,T) **alors**
    retourner p
  fin si
fin tant que

Complexité

Complexité en moyenne $O(T \cdot k^4)$

Validité

Probabilité d'erreur $\rightsquigarrow \leq 4^{-T}$

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

  tant que VRAI **faire**
    $p \xleftarrow{\text{⚂⚃}} [2^{k-1}, 2^k]$ ▷ Algorithme de type « Atlantic City »
    si MILLER-RABIN(p,T) **alors**
      retourner p
    fin si
  fin tant que

Complexité

Complexité en moyenne $O(T \cdot k^4)$

Validité

Probabilité d'erreur $\rightsquigarrow \leq 4^{-T}$

Agrawal-Kayal-Saxena : PRIMALITÉ $\in \mathcal{P}$

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n.$$

Nous avons

$$\mathcal{P}_n(z) = 0 \pmod{n} \text{ sssi } n \text{ est premier}$$

- 2002, M. Agrawal, N. Kayal, N. Saxena
- Premier algorithme déterministe pour PRIMALITÉ

Complexité

$O(\log(n)^{12}) \rightsquigarrow O(\log(n)^{10.5}) \rightsquigarrow O(\log(n)^{7.5}) \rightsquigarrow O(\log(n)^{6})$

Agrawal-Kayal-Saxena : PRIMALITÉ $\in \mathcal{P}$

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n.$$

Nous avons

$$\mathcal{P}_n(z) = 0 \pmod{n} \text{ sssi } n \text{ est premier}$$

- 2002, M. Agrawal, N. Kayal, N. Saxena
- Premier algorithme déterministe pour PRIMALITÉ

Complexité

$O(\log(n)^{12}) \rightsquigarrow O(\log(n)^{10.5}) \rightsquigarrow O(\log(n)^{7.5}) \rightsquigarrow O(\log(n)^{6})$

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

tant que VRAI **faire**
  $p \longleftarrow [2^{k-1}, 2^k]$
  si AKS(p) **alors**
    retourner p
  fin si
fin tant que

Complexité

Complexité en moyenne $O(k^7)$

Algorithme de type « Las Vegas »

Génération de nombres premiers

Entrée: $k \in \mathbb{N}$, $k \geq 1$
Sortie: $p \in \mathbb{P} \cap [2^{k-1}, 2^k]$

tant que VRAI **faire**
  $p \longleftarrow [2^{k-1}, 2^k]$
  si $\mathrm{AKS}(\mathrm{p})$ **alors**
    retourner p
  fin si
fin tant que

Complexité

Complexité en moyenne $O(k^7)$

Algorithme de type « Las Vegas »

Table des matières

Identité polynomiale

IDENTITÉ POLYNOMIALE

- ENTRÉE : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- SORTIE : VRAI si $P_1 = P_2$ et FAUX sinon

- polynômes égaux $\neq$ fonctions associées égales
- **Exemple :** sur $\mathbb{Z}/p\mathbb{Z}$ (avec p premier),

$$P_1(X) = X^p - X \text{ et } P_2(X) = 0$$

Identité polynomiale

IDENTITÉ POLYNOMIALE

- ENTRÉE : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- SORTIE : VRAI si $P_1 = P_2$ et FAUX sinon

- polynômes égaux $\neq$ fonctions associées égales
- **Exemple :** sur $\mathbb{Z}/p\mathbb{Z}$ (avec p premier),

$$P_1(X) = X^p - X \text{ et } P_2(X) = 0$$

Tableaux de coefficients

Identité polynomiale

- Entrée : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- Sortie : vrai si $P_1 = P_2$ et faux sinon

- Tableaux de longueur $\binom{n+d}{d} = \binom{n+d}{n}$
- Algorithme naïf de complexité $O\left(\binom{n+d}{d}\right)$

Tableaux de coefficients

IDENTITÉ POLYNOMIALE

- ENTRÉE : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- SORTIE : VRAI si $P_1 = P_2$ et FAUX sinon

- Tableaux de longueur $\binom{n+d}{d} = \binom{n+d}{n}$

- Algorithme naïf de complexité $O\left(\binom{n+d}{d}\right)$

Tableaux de coefficients

Identité polynomiale

- Entrée : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- Sortie : vrai si $P_1 = P_2$ et faux sinon

- Tableaux de longueur $\binom{n+d}{d} = \binom{n+d}{n}$
- Algorithme naïf de complexité $O\left(\binom{n+d}{d}\right)$

Listes degrés/coefficients

IDENTITÉ POLYNOMIALE

- ENTRÉE : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- SORTIE : VRAI si $P_1 = P_2$ et FAUX sinon

- Listes de longueur $\ell \leq \binom{n+d}{d}$
- Algorithme de complexité $O(\ell \log \ell)$

Listes degrés/coefficients

Identité polynomiale

- Entrée : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- Sortie : vrai si $P_1 = P_2$ et faux sinon

- Listes de longueur $\ell \leq \binom{n+d}{d}$
- Algorithme de complexité $O(\ell \log \ell)$

Listes degrés/coefficients

Identité polynomiale

- Entrée : P_1, P_2 deux polynômes degré $\leq d$ en n variables (définis sur un corps $\mathbb{K}$)
- Sortie : vrai si $P_1 = P_2$ et faux sinon

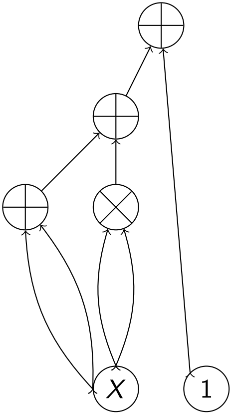
- Listes de longueur $\ell \leq \binom{n+d}{d}$
- Algorithme de complexité $O(\ell \log \ell)$

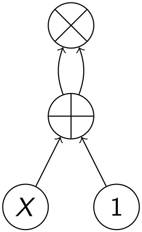
Circuits arithmétiques

$$(1 + z)^n \stackrel{?}{=} 1 - z^n \bmod n.$$

Circuits arithmétiques

$$(1+z)^n \stackrel{?}{=} 1 - z^n \bmod n.$$





Déterminant

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix}$$

$$\det(V) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Déterminant

$$V = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix}$$

$$\det(V) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Déterminant

$$C = \begin{bmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{bmatrix}$$

$$\det(C) = \prod_{j=0}^{n-1} (c_0 + c_{n-1}\omega^j + c_{n-2}\omega^{2j} + \cdots + c_1\omega^{(n-1)j}).$$

avec $\omega = \exp\left(\frac{2\pi i}{n}\right)$ une racine primitive n-ième de l'unité

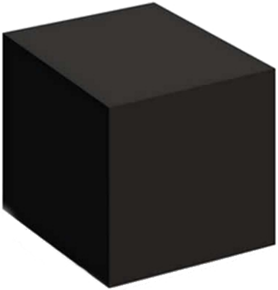
Déterminant

$$C = \begin{bmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{bmatrix}$$

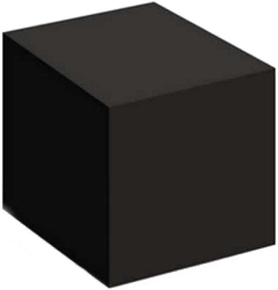
$$\det(C) = \prod_{j=0}^{n-1} (c_0 + c_{n-1}\omega^j + c_{n-2}\omega^{2j} + \cdots + c_1\omega^{(n-1)j}).$$

avec $\omega = \exp\left(\frac{2\pi i}{n}\right)$ une racine primitive n-ième de l'unité

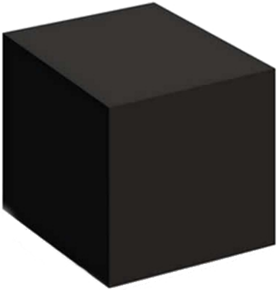
Boite noire



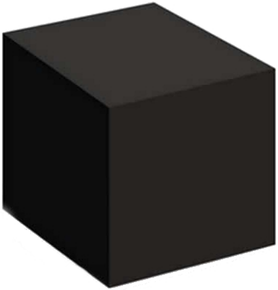
Boite noire

$(\alpha_1, \ldots, \alpha_n) \longrightarrow$ 

Boite noire

$(\alpha_1, \ldots, \alpha_n) \longrightarrow$  $\longrightarrow P(\alpha_1, \ldots, \alpha_n)$

Boite noire

$(\alpha_1, \ldots, \alpha_n) \longrightarrow$  $\longrightarrow P(\alpha_1, \ldots, \alpha_n)$

- $P = P_1 - P_2 \rightsquigarrow$ décider si $P = 0$
  (avec accès à son évaluation en « boite noire »)

Lemme de Schwartz-Zippel

Lemme de Schwartz-Zippel

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[x_1, \ldots, x_n]$

- n variables
- degré total $d \geq 1$
- non nul

Soit $S \subseteq \mathbb{K}$ un ensemble fini avec $\#S = s$.

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1, \ldots, r_n) = 0) \leq \frac{d}{s}$$

pour $(r_1, \ldots, r_n)$ tiré uniformément aléatoirement dans S^n

Lemme de Schwartz-Zippel

Lemme de Schwartz-Zippel

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[x_1, \ldots, x_n]$, degré total $d \geq 1$.
Soit $S \subseteq \mathbb{K}$ un ensemble fini avec $\#S = s$.

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1, \ldots, r_n) = 0) \leq \frac{d}{s}$$

- 1980, J. Schwartz – 1979, R.Zippel
- 1978, R. A. DeMillo, R. J. Lipton
- 1922, Ø. Ore (corps finis)
- `https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/`

Lemme de Schwartz-Zippel

Lemme de Schwartz-Zippel

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[x_1, \ldots, x_n]$, degré total $d \geq 1$.
Soit $S \subseteq \mathbb{K}$ un ensemble fini avec $\#S = s$.

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1, \ldots, r_n) = 0) \leq \frac{d}{s}$$

- 1980, J. Schwartz – 1979, R.Zippel
- 1978, R. A. DeMillo, R. J. Lipton
- 1922, Ø. Ore (corps finis)
- https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/

Lemme de Schwartz-Zippel

Lemme de Schwartz-Zippel

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[x_1, \ldots, x_n]$, degré total $d \geq 1$.
Soit $S \subseteq \mathbb{K}$ un ensemble fini avec $\#S = s$.

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1, \ldots, r_n) = 0) \leq \frac{d}{s}$$

- 1980, J. Schwartz – 1979, R.Zippel
- 1978, R. A. DeMillo, R. J. Lipton
- 1922, Ø. Ore (corps finis)
- `https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/`

Lemme de Schwartz-Zippel - Démonstration

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1,\ldots,r_n)=0) \leq \frac{d}{s}$$

Démonstration par récurrence sur n

- $n = 1$: P polynôme univarié, non nul, défini sur un corps
  $\rightsquigarrow$ au plus d racines dans $\mathbb{K}$
  $\rightsquigarrow$ au plus d racines dans S

$$\mathbb{P}_{r\in S}(P(r)=0) \leq \frac{d}{s}$$

Lemme de Schwartz-Zippel - Démonstration

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1,\ldots,r_n)=0) \le \frac{d}{s}$$

Démonstration par récurrence sur n

- Supposons le résultat montré pour tout entier $1 \le j \le n-1$
  Posons
  $$P(x_1,\ldots,x_n) = \sum_{i=0}^{d} x_1^i \cdot P_i(x_2,\ldots,x_n).$$
  Puisque P est non nul, il existe au moins un entier i tel que $P_i \neq 0$. Posons $i^\star$ le plus grand entier de $\{1,\ldots,d\}$ tel que $P_{i^\star} \neq 0$.
  $$P(x_1,\ldots,x_n) = \sum_{i=0}^{i^\star} x_1^i \cdot P_i(x_2,\ldots,x_n).$$

Lemme de Schwartz-Zippel - Démonstration

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1,\ldots,r_n)=0) \leq \frac{d}{s}$$

Démonstration par récurrence sur n

- Nous avons $\deg(P_{i^\star}) \leq d - i^\star$
  Par l'hypothèse de récurrence, nous avons

$$\begin{aligned}\#\{(r_2,\ldots,r_n)\in S^{n-1} | P_{i^\star}(r_2,\ldots,r_n)=0\} &\leq \frac{d-i^\star}{s}s^{n-1}\\ &= (d-i^\star)s^{n-2}\end{aligned}$$

  Par ailleurs si $P_{i^\star}(r_2,\ldots,r_n)\neq 0$, le nombre de r_1 tel que $P(r_1,\ldots,r_n)=0$ est majoré par $i^\star$ puisque

$$P(x_1,\ldots,x_n) = \sum_{i=0}^{i^\star} x_1^i \cdot P_i(x_2,\ldots,x_n).$$

Lemme de Schwartz-Zippel - Démonstration

$$\mathbb{P}_{(r_1,\ldots,r_n)\in S^n}(P(r_1,\ldots,r_n)=0) \leq \frac{d}{s}$$

Démonstration par récurrence sur n

- Nous avons :

$$\begin{aligned}
&\#\{(r_1,r_2,\ldots,r_n) \in S^{n-1} | P(r_2,\ldots,r_n)=0\} \\
&\leq i^\star \cdot \#\{(r_2,\ldots,r_n) \in S^{n-1} | P_{i^\star}(r_2,\ldots,r_n) \neq 0\} \\
&\quad + s \cdot \{(r_2,\ldots,r_n) \in S^{n-1} | P_{i^\star}(r_2,\ldots,r_n) = 0\} \\
&\leq i^\star \cdot s^{n-1} + s \cdot (d - i^\star) s^{n-2} \\
&\leq d s^{n-1}
\end{aligned}$$

$\square$

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
(avec accès en « boite noire »)
Sortie: Non nul ou Nul

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
$(r_1, \ldots, r_n) \xleftarrow{\text{⚂⚃}} S^n$
si $P(r_1, \ldots, r_n) \neq 0$ **alors**
  retourner Non nul
sinon
  retourner Nul
fin si

Complexité

Nombres d'évaluations :

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \dots, x_n]$, de degré au plus $d \geq 1$
(avec accès en « boite noire »)
Sortie: NON NUL ou NUL

$S \subseteq \mathbb{K}$ avec $\#S = s > d$

$(r_1, \dots, r_n) \xleftarrow{} S^n$

si $P(r_1, \dots, r_n) \neq 0$ **alors**

  retourner NON NUL

sinon

  retourner NUL

fin si

Complexité

Nombres d'évaluations : $O(1)$

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
(avec accès en « boite noire »)
Sortie: NON NUL ou NUL

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
$(r_1, \ldots, r_n) \xleftarrow{\quad} S^n$
si $P(r_1, \ldots, r_n) \neq 0$ **alors**
  retourner NON NUL
sinon
  retourner NUL
fin si

Complexité

Nombres d'évaluations : $O(1)$

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
(avec accès en « boite noire »)
Sortie: $\textsc{Non nul}$ ou $\textsc{Nul}$

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
$(r_1, \ldots, r_n) \longleftarrow S^n$
si $P(r_1, \ldots, r_n) \neq 0$ **alors**
  retourner $\textsc{Non nul}$
sinon
  retourner $\textsc{Nul}$
fin si

Complexité

Nombres d'évaluations : $O(1)$

Validité

Probabilité d'erreur : $\leq d/s < 1$

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
Sortie: Non nul ou Nul

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
pour i de 1 à T **faire**
  $(r_1, \ldots, r_n) \longleftarrow S^n$
  si $P(r_1, \ldots, r_n) \neq 0$ **alors**
    retourner Non nul
  fin si
fin pour
retourner Nul

Complexité

Nombres d'évaluations :

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
Sortie: NON NUL ou NUL

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
pour i de 1 à T **faire**
  $(r_1, \ldots, r_n) \xleftarrow{\text{⚂⚃}} S^n$
  si $P(r_1, \ldots, r_n) \neq 0$ **alors**
    retourner NON NUL
  fin si
fin pour
retourner NUL

Complexité

Nombres d'évaluations : $O(T)$

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \dots, x_n]$, de degré au plus $d \geq 1$
Sortie: NON NUL ou NUL

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
pour i de 1 à T **faire**
  $(r_1, \dots, r_n) \xleftarrow{\text{⚂⚃}} S^n$
  si $P(r_1, \dots, r_n) \neq 0$ **alors**
    retourner NON NUL
  fin si
fin pour
retourner NUL

Complexité

Nombres d'évaluations : $O(T)$

Validité

Probabilité d'erreur :

Algorithme de type Monte-Carlo

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
Sortie: Non nul ou Nul

$S \subseteq \mathbb{K}$ avec $\#S = s > d$
pour i de 1 à T **faire**
$(r_1, \ldots, r_n) \xleftarrow{\quad} S^n$
si $P(r_1, \ldots, r_n) \neq 0$ **alors**
retourner Non nul
fin si
fin pour
retourner Nul

Complexité

Nombres d'évaluations : $O(T)$

Validité

Probabilité d'erreur : $\leq (d/s)^T$

Algorithme de type Las-Vegas

Entrée: $P \in \mathbb{K}[x_1, \ldots, x_n]$, de degré au plus $d \geq 1$
(avec accès en « boite noire »)
Sortie: Non nul ou Nul

$S \subseteq \mathbb{K}$ avec $\#S = 2d$
$E \leftarrow S^n$
tant que $E \neq \emptyset$ **faire**
  $(r_1, \ldots, r_n) \xleftarrow{\text{⚂⚃}} E$
  $E \leftarrow E \setminus \{(r_1, \ldots, r_n)\}$
  si $P(r_1, \ldots, r_n) \neq 0$ **alors**
    retourner Non nul
  fin si
fin tant que
retourner Nul

Algorithme de type Las-Vegas

Validité

Probabilité d'erreur :

Algorithme de type Las-Vegas

Validité

Probabilité d'erreur : 0

Algorithme de type Las-Vegas

Validité

Probabilité d'erreur : 0

Complexité

Nombres d'évaluations :

Algorithme de type Las-Vegas

Validité

Probabilité d'erreur : 0

Complexité

Nombres d'évaluations :

- si $P \neq 0$, en moyenne $2 \rightsquigarrow O(1)$
- si $P = 0$, $O(d^n)$

Dans le pire des cas, complexité exponentielle !

Test de primalité ?

Considérons

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n.$$

Nous avons

$$\mathcal{P}_n(z) = 0 \pmod{n} \text{ sssi } n \text{ est premier}$$

Mais on ne peut pas appliquer le lemme de Schwartz–Zippel

- $(\mathbb{Z}/n\mathbb{Z})$ pas nécessairement un corps
- $\deg(P) = n \rightsquigarrow$ probabilité inférieure à 1 !

Remarque

Agrawal et Biswas ont proposé une méthode plus sophistiquée en vérifiant cette égalité modulo un polynôme aléatoire unitaire de petit degré (2008, M. Agrawal, S. Biswas – *cf.* Compléments du TD)

Test de primalité ?

Considérons

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n.$$

Nous avons

$$\mathcal{P}_n(z) = 0 \pmod{n} \text{ ssi } n \text{ est premier}$$

Mais on ne peut pas appliquer le lemme de Schwartz–Zippel

- $(\mathbb{Z}/n\mathbb{Z})$ pas nécessairement un corps
- $\deg(P) = n \rightsquigarrow$ probabilité inférieure à 1 !

Remarque

Agrawal et Biswas ont proposé une méthode plus sophistiquée en vérifiant cette égalité modulo un polynôme aléatoire unitaire de petit degré (2008, M. Agrawal, S. Biswas – *cf.* Compléments du TD)