Introduction à la cryptographie

Vanessa VITSE

Université Grenoble Alpes

M1 Maths 2021

Section 3

Générateurs de nombres premiers et tests de primalité

Rappels sur la distribution des nombres premiers

Il existe une infinité de nombres premiers, mais quelle est la probabilité qu'un nombre tiré au hasard soit premier ?

Rappels sur la distribution des nombres premiers

Il existe une infinité de nombres premiers, mais quelle est la probabilité qu'un nombre tiré au hasard soit premier ?

Hadamard and de la Vallée Poussin, 1896

Pour $n \geqslant 17$,

$$\frac{n}{\ln n} \leqslant \pi(n) \leqslant 2\frac{n}{\ln n}.$$

$\rightarrow$ très bonne proba (en $1/\ln n$)

Rappels sur la distribution des nombres premiers

Il existe une infinité de nombres premiers, mais quelle est la probabilité qu'un nombre tiré au hasard soit premier ?

Hadamard and de la Vallée Poussin, 1896

Pour $n \geqslant 17$,

$$\frac{n}{\ln n} \leqslant \pi(n) \leqslant 2\frac{n}{\ln n}.$$

$\rightarrow$ très bonne proba (en $1/\ln n$)

Plus précisément,

$$\pi(n) \underset{n\to\infty}{\sim} \int_2^n \frac{dt}{\ln(t)}.$$

Exemple : environ 1 nombre sur 21 est premier au voisinage de $n = 1\,000\,000\,000$.

Rappels sur la distribution des nombres premiers

Il existe une infinité de nombres premiers, mais quelle est la probabilité qu'un nombre tiré au hasard soit premier ?

Hadamard and de la Vallée Poussin, 1896

Pour $n \geqslant 17$,

$$\frac{n}{\ln n} \leqslant \pi(n) \leqslant 2\frac{n}{\ln n}.$$

$\rightarrow$ très bonne proba (en $1/\ln n$)

Plus précisément,

$$\pi(n) \underset{n\to\infty}{\sim} \int_2^n \frac{dt}{\ln(t)}.$$

Exemple : environ 1 nombre sur 21 est premier au voisinage de $n = 1\,000\,000\,000$.

besoin de tests de primalité efficaces avec certificat

Premier test de primalité : “trial division”

But : déterminer si n est premier ou pas

Premier test de primalité : “trial division”

But : déterminer si n est premier ou pas
on teste si tous les premiers $p \leqslant \sqrt{n}$ divise n ;
s’il n’en existe pas, n est premier

Propriété

Si $n \geqslant 0$ est un entier composé, alors il existe un nombre premier p tel que $p \leqslant \sqrt{n}$ et $p|n$.

Premier test de primalité : “trial division”

But : déterminer si n est premier ou pas
on teste si tous les premiers $p \leqslant \sqrt{n}$ divise n ;
s'il n'en existe pas, n est premier

Propriété

Si $n \geqslant 0$ est un entier composé, alors il existe un nombre premier p tel que $p \leqslant \sqrt{n}$ et $p|n$.

Exemple : $n = 10007$ est premier car tous les premiers inférieurs à 100 (faire un *crible d'Ératosthène* pour les obtenir) ne sont pas des diviseurs

Premier test de primalité : “trial division”

But : déterminer si n est premier ou pas
on teste si tous les premiers $p \leqslant \sqrt{n}$ divise n ;
s'il n'en existe pas, n est premier

Propriété

Si $n \geqslant 0$ est un entier composé, alors il existe un nombre premier p tel que $p \leqslant \sqrt{n}$ et $p|n$.

Exemple : $n = 10007$ est premier car tous les premiers inférieurs à 100 (faire un *crible d'Ératosthène* pour les obtenir) ne sont pas des diviseurs

Complexité exponentielle !

coût $\simeq \sqrt{n}/\ln(\sqrt{n})$ divisions pour tester si n est premier
$\rightarrow$ si $n \simeq 10^{300}$ (taille des premiers dans RSA), il faut faire 2.9^{147} tests de divisions !!

Tests de pseudo-primalité

Définition

Un test de pseudo-primalité est un algorithme (non-déterministe) tel que, étant donné n, il retourne `True` si n est premier, et `True` ou `False` si n est composé.

- seule la sortie `False` permet de répondre avec certitude
- très efficaces et largement utilisés
- fournissent pas toujours des *certificats de primalité ou non-primalité* ($\neq$ tests déterministes).

Tests de pseudo-primalité

Définition

Un test de pseudo-primalité est un algorithme (non-déterministe) tel que, étant donné n, il retourne `True` si n est premier, et `True` ou `False` si n est composé.

- seule la sortie `False` permet de répondre avec certitude
- très efficaces et largement utilisés
- fournissent pas toujours des *certificats de primalité ou non-primalité* ($\neq$ tests déterministes).

Théorème d'Euler-Fermat

Si p est premier et $a \in \mathbb{Z}$, alors $a^p = a \bmod p$.

(application directe de Lagrange au groupe $\mathbb{Z}/p\mathbb{Z}^*$)

Test de pseudo-primalité de Fermat

La contraposée d'Euler-Fermat donne un certificat de non-primalité

Test de Fermat

S'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ t.q. $a^n \neq a$, alors n est composé.

Exemples :

- $2^{25009997} = 2384555 \bmod 25009997$ donc 25009997 n'est pas premier et 2 fournit un certificat

Test de pseudo-primalité de Fermat

La contraposée d'Euler-Fermat donne un certificat de non-primalité

Test de Fermat

S'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ t.q. $a^n \neq a$, alors n est composé.

Exemples :

- $2^{25009997} = 2384555 \bmod 25009997$ donc 25009997 n'est pas premier et 2 fournit un certificat
- $2^{341} = 2 \bmod 341$ ne nous apprend rien mais $3^{341} = 168 \bmod 341$ fournit un certificat

Test de pseudo-primalité de Fermat

La contraposée d'Euler-Fermat donne un certificat de non-primalité

Test de Fermat

S'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ t.q. $a^n \neq a$, alors n est composé.

Exemples :

- $2^{25009997} = 2384555 \bmod 25009997$ donc 25009997 n'est pas premier et 2 fournit un certificat
- $2^{341} = 2 \bmod 341$ ne nous apprend rien mais $3^{341} = 168 \bmod 341$ fournit un certificat
- pour $n = 561$ aucune valeur de a ne peut fournir un certificat...

Test de pseudo-primalité de Fermat

La contraposée d'Euler-Fermat donne un certificat de non-primalité

Test de Fermat

S'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ t.q. $a^n \neq a$, alors n est composé.

Exemples :

- $2^{25009997} = 2384555 \bmod 25009997$ donc 25009997 n'est pas premier et 2 fournit un certificat
- $2^{341} = 2 \bmod 341$ ne nous apprend rien mais $3^{341} = 168 \bmod 341$ fournit un certificat
- pour $n = 561$ aucune valeur de a ne peut fournir un certificat...

Remarque : $H = \{a \in \mathbb{Z}/n\mathbb{Z}^\times : a^{n-1} = 1\} < (\mathbb{Z}/n\mathbb{Z})^\times$
donc si H ss-groupe strict, alors $|H| \leqslant \frac{\varphi(n)}{2} \leqslant \frac{n}{2}$ d'où $\mathbb{P}(a^{n-1} \neq 1) \geqslant 1/2$

Test de pseudo-primalité de Fermat

La contraposée d'Euler-Fermat donne un certificat de non-primalité

Test de Fermat

S'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ t.q. $a^n \neq a$, alors n est composé.

Exemples :

- $2^{25009997} = 2384555 \bmod 25009997$ donc 25009997 n'est pas premier et 2 fournit un certificat
- $2^{341} = 2 \bmod 341$ ne nous apprend rien mais $3^{341} = 168 \bmod 341$ fournit un certificat
- pour $n = 561$ aucune valeur de a ne peut fournir un certificat...

Remarque : $H = \{a \in \mathbb{Z}/n\mathbb{Z}^\times : a^{n-1} = 1\} < (\mathbb{Z}/n\mathbb{Z})^\times$
donc si H ss-groupe strict, alors $|H| \leqslant \frac{\varphi(n)}{2} \leqslant \frac{n}{2}$ d'où $\mathbb{P}(a^{n-1} \neq 1) \geqslant 1/2$

Problème si $H = (\mathbb{Z}/n\mathbb{Z})^\times$

Test de pseudo-primalité de Fermat

Nombres de Carmichael

Un nombre de Carmichael est un entier composé n tel que

$$\forall a \in \mathbb{Z}, a^n = a \bmod n.$$

- il en existe une infinité (Alford-Granville-Pomerance 90's)
- mais ils sont très rares (donc improbable d'en tirer un au hasard)
- sauf que qq de malveillant pourrait en avoir usage en crypto...

Autres tentatives...

On peut utiliser le critère suivant

Proposition

Un entier n est premier si et seulement si $\varphi(n) = n - 1$.

- sens direct par contraposition : $\varphi(p^k) = p^k - p^{k-1} < p^k - 1$ et $\varphi(ab) \leqslant (a-1)(b-1) < ab - 1$
- MAIS calculer $\varphi(n)$ est aussi dur que factoriser n (exo si $n = pq$)

Autres tentatives...

On peut utiliser le critère suivant

Proposition

Un entier n est premier si et seulement si $\varphi(n) = n - 1$.

- sens direct par contraposition : $\varphi(p^k) = p^k - p^{k-1} < p^k - 1$ et $\varphi(ab) \leqslant (a-1)(b-1) < ab - 1$
- MAIS calculer $\varphi(n)$ est aussi dur que factoriser n (exo si $n = pq$)

Vers Miller-Rabin...

Soit p un entier impair premier et $s, t \in \mathbb{N}^*$ avec t impair tel que $p = 2^s t + 1$.
Soit a un entier non divisible par p. Alors, l'une des pptés suivantes est satisfaite :

- P1 $a^t = 1 \bmod p$
- P2 $a^{2^i t} = -1 \bmod p$ pour un certain $0 \leqslant i < s$

Test de primalité de Miller-Rabin

Définition

Un entier a est appelé *témoin de non-primalité* d'un entier impair n si $a \neq 0 \bmod n$ et (P_1) **et** (P_2) ne sont pas satisfaites

Exemple : avec $n = 561$ et $a = 5$. On a $n - 1 = 560 = 2^4 \times 35$ et

- $5^{35} = 23 \neq \pm 1 \bmod 561$
- $5^{35 \cdot 2} = (23)^2 = 529 \neq -1 \bmod 561$
- $5^{35 \cdot 2^2} = (529)^2 = 463 \neq -1 \bmod 561$
- $5^{35 \cdot 2^3} = (463)^2 = 67 \neq -1 \bmod 561.$

Donc 5 est un témoin de non-primalité de $n = 561$

Test de primalité de Miller-Rabin

Algorithm 1: Test de primalité de Miller-Rabin

Input : n un entier impair
Output: true si n probablement premier, false si n n'est pas premier

```
a ∈ {1, ..., n − 1} entier aléatoire
s, t tel que n = 2^s t + 1 et t impair
b ← a^t mod n
if b == 1 then return True
for i = 0, ..., s − 1 do
    if b == −1 then return True
    b ← b^2
return False
```

Test de primalité de Miller-Rabin

Algorithm 1: Test de primalité de Miller-Rabin

Input : n un entier impair
Output: true si n probablement premier, false si n n'est pas premier
$a \in \{1, \ldots, n-1\}$ entier aléatoire
s, t tel que $n = 2^s t + 1$ et t impair
$b \leftarrow a^t \bmod n$
if $b == 1$ **then return** True
for $i = 0, \ldots, s-1$ **do**
  if $b == -1$ **then return** True
  if $b == 1$ **then return** Factorisation !
  $b \leftarrow b^2$
return False

Exercice : Montrer que l'on peut interrompre la boucle si $b = 1$ et qu'on a alors une factorisation de n.

Test de primalité de Miller-Rabin

Question naturelle : est-ce qu'un entier composé possède (ou pas) beaucoup de témoins ?

Test de primalité de Miller-Rabin

Question naturelle : est-ce qu'un entier composé possède (ou pas) beaucoup de témoins ?

Théorème

Soit n un entier composé impair.
La probabilité qu'un entier aléatoire $a \in \{1, \ldots, n-1\}$ soit un témoin de non-primalité pour n est supérieure à $3/4$.

- si n n'est pas premier et que l'on tire aléatoirement k entiers dans $\{1, \ldots, n-1\}$, la probabilité de ne pas trouver de témoin de non-primalité est inférieure à $1/4^k$ donc très faible
- si n n'est pas premier, on pourra rien prouver (sauf si l'on teste plus de $1/4$ de potentiels témoins, impraticable !)

Efficacité de Miller-Rabin

Théorème de Damgård-Landrock-Pomerance (admis)

Soit n un entier impair aléatoire dans $[2^k; 2^{k+1}]$. Soit a un entier aléatoire dans $\{1, \dots, n-1\}$.
Si a n'est pas un témoin de non-primalité de n, alors

$$\mathbb{P}(n \text{ est premier}) \geqslant 1 - k^2 \cdot 4^{2-\sqrt{k}}.$$

Efficacité de Miller-Rabin

Théorème de Damgård-Landrock-Pomerance (admis)

Soit n un entier impair aléatoire dans $[2^k; 2^{k+1}]$. Soit a un entier aléatoire dans $\{1, \ldots, n-1\}$.
Si a n'est pas un témoin de non-primalité de n, alors

$$\mathbb{P}(n \text{ est premier}) \geqslant 1 - k^2 \cdot 4^{2-\sqrt{k}}.$$

- si n grand entier aléatoire passe un seul test de Miller-Rabin, alors il est premier avec très bonne proba
  Ex : pour $k = 1024$, la proba est $\geqslant 1 - 2^{-40}$, donc astronomiquement proche de 1 si l'on répète le test
- Il existe des tests déterministes (le premier est AKS en 2003) de complexité polynomiale mais nettement moins efficaces.