TD N°4

Exercice 1 :

1) Basant sur la condition (i) de lemme 4.1, donner l'algorithme de temps polynomial probabiliste du test de primalité de fermât ?
2) Basant sur la condition (ii) de lemme 4.1, donner l'algorithme de temps polynomial probabiliste du test de primalité de Miller- Rabin ?

Solution :

1) L'algorithme de test de primalité de fermât.

Algorithm *The Fermat 'Almost Prime' Test.*

Input: an integer $n \geq 2$.
Algorithm:
choose $a \in_R \mathbb{Z}_n^+$
if $a^{n-1} = 1 \bmod n$
then output 'prime'
else output 'composite'.

Cet algorithme résout dans la plupart des cas notre problème. Si l'entrée est prime, elle produit certainement « premier ». Alors que si l'entrée est composée, mais pas un nombre de Carmichael, alors la proposition vue en cours implique qu'elle produira un « composé » avec une probabilité d'au moins la moitié.
Puisque cet algorithme est clairement à temps polynomial, nous aurions un algorithme de test de primalité très simple si les nombres de Carmichael n'existaient pas. Malheureusement, il existe une infinité de nombres tels que le suggère le théorème 4.3

2) L'algorithme de test de primalité de Miller.

Dans la condition (ii), nous avons décrit un deuxième type de témoin pour un nombre composé : le témoin de Miller. Le test de primalité de Miller – Rabin utilise à la fois des témoins de Fermat et de Miller.

Algorithm *The Miller–Rabin Primality Test.*

Input: an odd integer $n \geq 3$.
Algorithm:
choose $a \in_R \mathbb{Z}_n^+$
if $\gcd(a, n) \neq 1$ output 'composite'
let $n - 1 = 2^k m$, with m odd
if $a^m = 1 \bmod n$ output 'prime'
for $i = 0$ to $k - 1$
  if $a^{m \cdot 2^i} = -1 \bmod n$ then output 'prime'
next i
output 'composite'.

Exercice 2 : Supposons f ∈ Z [x_1,. . . , x_n] a un degré au plus k et n'est pas identiquement nul. Si a_1,. . . , a_n sont choisis indépendamment et uniformément au hasard parmi {1,. . . , N}.

Monter que

$$\Pr[f(a_1, \ldots, a_n) = 0] \leq \frac{k}{N}.$$

Solution :

Preuve: Nous utilisons l'induction sur n. Pour n = 1, le résultat est valable puisqu'un polynôme de degré au plus k dans une seule variable a au plus k racines. Alors laissez n> 1 et écrivez

$$f = f_0 + f_1 x_1 + f_2 x_1^2 + \cdots + f_t x_1^t,$$

où f_0,. . . f_t sont des polynômes en x_2, x_3,. . . x_n; f_t n'est pas identiquement nul et t ≥ 0. Si t = 0 alors f est un polynôme en n - 1 variables donc le résultat est vrai. Donc on peut supposer que 1 ≤ t ≤ k et f_t est de degré au plus k - t.

On note E_1 l'événement f (a_1,..., a_n) = 0 et E_2 l'événement f_t (a_2,..., a_n) = 0. À présent

$$\begin{aligned}\Pr[E_1] &= \Pr[E_1 \mid E_2] \Pr[E_2] + \Pr[E_1 \mid \text{not } E_2] \Pr[\text{not } E_2] \\ &\leq \Pr[E_2] + \Pr[E_1 \mid \text{not } E_2].\end{aligned}$$

Notre hypothèse inductive implique que

$$\Pr[E_2] = \Pr[f_t(a_2, \ldots, a_n) = 0] \leq \frac{(k - t)}{N},$$

puisque f_t a un degré au plus k - t.

aussi

$$\Pr[E_1 \mid \text{not } E_2] \leq \frac{t}{N}.$$

Ceci est vrai car a_1 est choisi indépendamment de $a_2,\ldots, a_n$, donc si $a_2,\ldots, a_n$ sont fixes et on sait que $f_t(a_2,\ldots a_n) = 0$ alors f est un polynôme en x_1 qui n'est pas identiquement nul. Donc f, en tant que polynôme dans x_1, a le degré t et a donc au plus t racines.

En mettant cela ensemble, nous obtenons

$$\Pr[f(a_1,\ldots,a_n) = 0] \leq \frac{k-t}{N} + \frac{t}{N} \leq \frac{k}{N}$$

Exercice 3 :

1) Montrer que P ⊆ RP ⊆ NP ?
2) Montrer Lemme 4.1 ?
3) Montrer la proposition 4.2 ?
4) Monter que l'algorithme de Miller- Rabin est probabiliste à temps polynomial ? déduire que le langage COMPOSÉ ∈ RP et PRIMIER ∈ co-RP ?

Solution :

1) Preuve : L'inclusion P ⊆ RP est trivial car une DTM est simplement un PTM qui ne jette jamais de pièces.

Pour voir que RP ⊆ NP ; soit L ∈ RP. Alors il existe un PTM M et un polynôme p(n) tels que si x ∈ L alors

$$\Pr[M \text{ accepts } x] \geq \frac{1}{2},$$

tandis que si x ∉ L alors

$$\Pr[M \text{ accepts } x] = 0.$$

Donc si x ∈ L alors il existe certainement au moins une chaîne y ∈ Σ_0^* de longueur au plus

p (| x |) telle que M accepte x en utilisant y comme bits aléatoires sur sa bande de tirage au sort. De plus, si x ∉ L alors une telle chaîne y n'existe pas. Ainsi, nous pouvons construire un DTM qui à l'entrée x y imite le calcul de M avec l'entrée x et des « bits aléatoires » donnés par y. Par l'argument ci-dessus, cette machine montre que L ∈ NP et donc RP ⊆ NP.

2) Preuve:
   Soit

   $$\mathbb{Z}_n^+ = \{a \in \mathbb{Z}_n \mid a \neq 0\}.$$

   Si p est premier alors $a^{p-1} = 1 \bmod p$ pour tout $a \in \mathbb{Z}_p^+$, par le petit théorème de Fermat. Donc si (i) est vrai alors n est composite.

Si (ii) est vrai alors soit b le dernier entier de la séquence a^m, a^{2m},. . . qui n'est pas congru à 1 mod n. Alors $b^2 = 1 \bmod n$ mais $b \neq \pm 1 \bmod n$. Donc b + 1 et b - 1 sont des facteurs non triviaux de n donc n est composite.

Si $a \in \mathbb{Z}_n^+$ satisfait la condition (i) du lemme 4.1 alors on l'appelle un témoin de Fermat pour la composition de n, tandis que s'il satisfait la condition (ii) du lemme 4.1, on l'appelle un témoin de Miller.

De nombreux entiers composés ont beaucoup de témoins de Fermat. Malheureusement, il en existe qui en ont très peu. Pour un entier composé n, nous définissons l'ensemble des témoins de Fermat pour n comme étant

$$F_n = \{a \in \mathbb{Z}_n^+ \mid a \text{ is a Fermat witness for } n\}.$$

Notez que si $a \in \mathbb{Z}_n^+$ n'est pas un témoin de Fermat alors $a^{n-1} = 1 \bmod n$ et donc il existe $k \in \mathbb{Z}$ tel que

$$a^{n-1} - kn = 1$$

Or, puisque pgcd (a, n) divise le côté gauche de cette équation, nous devons avoir

pgcd (a, n) = 1. Par conséquent, tout $a \in \mathbb{Z}_n^+$ qui n'est pas premier avec n est un témoin de Fermat pour n .

3) Preuve: Rappelons que l'ensemble des entiers inférieurs à un co-premier d'un entier n forme un groupe multiplicatif $\mathbb{Z}_n^* = \{1 \leq a < n \mid \text{pgcd}(a, n) = 1\}$.

   Considérons l'ensemble $B = \mathbb{Z}_n^* \setminus F_n$, donc

   $$B = \{a \in \mathbb{Z}_n^* \mid a^{n-1} = 1 \bmod n\}$$

   Ceci est facilement perçu comme étant un sous-groupe de $\mathbb{Z}_n^*$ puisque
   (i) si a, b ∈ B alors $(ab)^{n-1} = a^{n-1}b^{n-1} = 1 \cdot 1 = 1 \bmod n$, donc ab ∈ B;
   (ii) si a ∈ B alors $(a^{-1})^{n-1} = (a^{n-1})^{-1} = 1^{-1} = 1 \bmod n$, d'où $a^{-1} \in B$;
   (iii) $1^{n-1} = 1 \bmod n$, donc 1 ∈ B.

   Donc B est un sous-groupe de $\mathbb{Z}_n^*$. Puisque n est composé mais pas un nombre de Carmichael, il existe $b \in \mathbb{Z}_n^* \setminus B$. Donc B est un sous-groupe propre de $\mathbb{Z}_n^*$ et donc par le théorème de Lagrange, | B | est un diviseur propre de $|\mathbb{Z}_n^*|$. D'où
   | B | ≤ (n - 1) / 2 et ainsi

   $$|F_n| = |\mathbb{Z}_n^+| - |B| > n/2$$

4) Preuve : Le test de Miller – Rabin est clairement un algorithme de temps polynomial probabiliste car il implique des opérations de base telles que la multiplication, le calcul des plus grands diviseurs communs et l'exponentiation en mod qui peuvent tous être effectués en temps polynomial.
Pour voir que (i) est vrai, supposons que n est premier. Alors pour tout a ∈ $\mathbb{Z}_n^+$, nous avons gcd (a, n) = 1 et donc l'algorithme ne peut pas afficher 'composé' à la ligne 2. La seule autre façon de produire 'composé' est si $a^m \neq 1 \bmod n$ et $a^{m2^i} \neq -1 \bmod n$ pour tout $0 \leq i \leq k - 1$. Dans ce cas, soit $a^{n-1} = 1 \bmod n$ et donc a est un témoin de Fermat pour n, soit $a^{n-1} = 1 \bmod n$ et donc a est un témoin de Miller pour n. Mais d'après le lemme 4.1, cela est impossible, puisque n est premier.
Il reste à prouver (ii). Nous considérons deux cas.

Cas 1 : n est composé mais pas un nombre de Carmichael.
Supposons que l'algorithme affiche « premier ». Alors soit $a^m = 1 \bmod n$ ou $a^{m2^i} = -1 \bmod n$, pour un certain $0 \leq i \leq k - 1$. Dans les deux cas $a^{n-1} = 1 \bmod n$, donc a n'est pas un témoin de Fermat pour n. Cependant, par la proposition 4.2, nous savons que | Fn | > n / 2 et ainsi

Pr [l'algorithme produit « composé »] ≥ ½

Cas 2 : n est un nombre de Carmichael.

Nous considérons deux sous-cas selon que n est une puissance d'un nombre premier ou non. (Rappelons que n est une puissance d'un nombre premier si $n = p^k$, avec p premier et $k \geq 1$.)

Cas 2a : n n'est pas une puissance d'un nombre premier.

Définir

$$t = \max\left\{0 \leq i \leq k-1 \mid \exists a \in \mathbb{Z}_n^* \text{ such that } a^{m \cdot 2^i} = -1 \bmod n\right\}$$

Et

$$B_t = \left\{a \in \mathbb{Z}_n^* \mid a^{m \cdot 2^t} = \pm 1 \bmod n\right\}$$

Notez que si $a \notin B_t$ alors l'algorithme affiche « composé ». Puisque si l'algorithme produit « premier », alors soit $a^m = 1 \bmod n$, soit, selon la définition de t, il existe $0 \leq i \leq t$ tel que $a^{m2^i} = -1 \bmod n$. Dans les deux cas, cela impliquerait que $a^{m2^i} = \pm 1 \bmod n$
Il suffira donc de prouver que $|B_t| \leq |\mathbb{Z}_n^*| / 2$ pour compléter la preuve dans ce cas.
Or B_t est un sous-groupe de $\mathbb{Z}_n^*$ puisque les conditions suivantes sont vérifiées

(i) si a, b ∈ B_t alors $(ab)^{m \cdot 2^t} = a^{m \cdot 2^t} b^{m \cdot 2^t} = (\pm 1) \cdot (\pm 1) = \pm 1 \bmod n$, donc ab∈ B_t;

(ii) si a ∈ B_t alors $(a^{-1})^{m2^t} = (a^{m2^t})^{-1} = (\pm 1)^{-1} = \pm 1 \bmod n$, donc $a^{-1} \in B_t$;

(iii) $1^{m2^t} = 1 \bmod n$, donc 1 ∈ B_t.

Si nous pouvons montrer que $B_t \neq \mathbb{Z}_n^*$ alors nous aurons fini, puisque le théorème de Lagrange implique que $|B_t| \leq |\mathbb{Z}_n^*| / 2$.

La définition de t implique qu'il existe un $\in \mathbb{Z}_n^*$ tel que $a^{m2^t} = -1 \bmod n$. Comme $n \geq 3$ n'est pas une puissance d'un premier, nous pouvons factoriser n comme n = cd, avec $3 \leq c, d < n$ et pgcd (c, d) = 1. Le théorème du reste chinois implique qu'il existe $b \in \mathbb{Z}_n^*$ satisfaisant

$$b = a \bmod c,$$
$$b = 1 \bmod d.$$

Ces équations impliquent que $b \in \mathbb{Z}_n^*$. Cependant $b \notin B_t$, puisque

$$b^{m \cdot 2^t} = a^{m \cdot 2^t} = -1 \bmod c,$$
$$b^{m \cdot 2^t} = 1^{m \cdot 2^t} = 1 \bmod d,$$

Impliquent que $b^{m2^t} \neq \pm 1 \bmod n$. D'où $B_t \neq \mathbb{Z}_n^*$.

Cas 2b : n est une puissance d'un premier et un nombre de Carmichael. Aucun nombre de Carmichael n'est une puissance d'un premier (voir l'exercice 3 pour une preuve de cela). La preuve est donc complète.

Ce résultat montre que le langage COMPOSÉ $\in$ RP ou de manière équivalente que PRIMIER $\in$ co-RP

Il existe également un test de primalité probabiliste dû à Adleman et Huang (1987) qui montre que PRIME $\in$ RP. D' où PRIME $\in$ RP $\cap$ co-RP. Tout langage dans RP $\cap$ co-RP a en fait un algorithme probabiliste avec un temps d'exécution polynomial attendu qui a une probabilité nulle de faire une erreur. Cependant, nous savons maintenant que PRIME $\in$ P, ce qui implique tous les résultats mentionnés ci-dessus.