ÉNS de Lyon Option C
2018-2019

Tests de primalité

Exercice 1 —Nombres de Carmichael

1. Montrer que tout nombre de Carmichael est impair.

2. Soit $n \in \mathbb{N}$. On veut montrer que les conditions suivantes sont équivalentes :

(i) n est sans facteur multiple et $p-1$ divise $n-1$ pour tout facteur premier p de n

(ii) $a^n \equiv a[n]$ pour tout entier a

(iii) $a^{n-1} \equiv 1[n]$ pour tout entier a premier à n.

a. Montrer que (i) implique (ii) et que (ii) implique (iii).

b. Soit n vérifiant (iii). Supposons que pour un nombre premier p, p^2 divise n. On écrit $n = p^2 m$. Montrer que $1 + pm$ est d'ordre p modulo n. En déduire une contradiction.

c. Soit n vérifiant (iii). On écrit $n = p_1 \dots p_r$, où les p_i sont des nombres premiers distincts. Montrer qu'il existe $a \in [\![1, n]\!]$ tel que $a[p_i]$ soit une racine primitive $p_i - 1$-ième de l'unité pour tout i. En déduire que n vérifie (i).

3. Montrer que tout nombre de Carmichael est produit d'au moins trois nombres premiers distincts.

4. Soit $n \in \mathbb{N}$. Montrer que ou bien n ne possède aucun témoin de Fermat, ou bien il en possède au moins $\frac{n}{2}$.

Exercice 2 —Complexité du test de Miller-Rabin

Soit $n \in \mathbb{N}$. On écrit $n = 2^s t$ avec t impair. Soit $a \in [\![2, n-1]\!]$. On dit que a est un **témoin de Miller** (pour n) si $a^t \not\equiv 1[n]$ et $a^{2^i t} \not\equiv 1[n]$ pour tout $i \in [\![1, s-1]\!]$. On rappelle que si n est premier, il n'a pas de témoin de Miller et si n n'est pas premier, au moins les trois-quarts des $a \in [\![2, n-1]\!]$ sont des témoins de Miller.

1. Soit $\epsilon \in]0, 1]$. Soit $n \in \mathbb{N}$. On tire un nombre $a \in [\![2, n-1]\!]$ au hasard et on teste si c'est un témoin de Miller. Majorer le nombre C de $a \in [\![1, n]\!]$ qu'il faut tester (avec remise) pour que si n est composé, la « probabilité » de n'avoir choisi aucun témoin de Miller soit inférieure à ϵ.

2. Majorer le coût en calcul d'un test de Miller-Rabin prenant en entrée un entier n et renvoyant « Vrai » si l'entier est composé avec probabilité $< \varepsilon$.

Exercice 3 —Recherche d'un nombre premier aléatoire

Soit m un entier. On cherche à obtenir un nombre premier aléatoire $\leq m$. On suppose qu'on dispose d'un test de primalité probabiliste, qui répond « Vrai » si l'entier est composé avec probabilité $< \varepsilon$. Si $n \in \mathbb{N}$, on note $C(n)$ le temps que met le test à renvoyer une réponse si l'entrée est inférieure ou égale à n.

On utilise la méthode suivante : on tire un nombre a au hasard dans $\{1, \ldots, m\}$. Si le test répond Vrai on renvoie a, sinon on recommence.

1. Majorer l'espérance du nombre de tirages nécessaires avant d'obtenir un a tel que le test réponde Vrai (on se rappellera que pour tout entier n, le nombre $\pi(n)$ de nombres premiers $\leq n$ est de l'ordre de $n/\log n$).

2. En déduire une majoration de l'espérance du temps que met le test à renvoyer un entier a.

3. Majorer la probabilité que l'entier renvoyé soit composé.

Exercice 4 —Test de primalité de Lucas-Lehmer pour les nombres de Mersenne

1. Soient a et $n \in \mathbb{N}_{\geq 2}$ tels que $a^n - 1$ est premier. Montrer que $a = 2$ et que n est premier.

Soient p un nombre premier impair et $M = 2^p - 1$. On pose $s_0 = 4$ et $s_{k+1} = s_k^2 - 2$ pour $k \in \mathbb{N}$. L'objectif est de démontrer le théorème suivant :

$(*)$ M est premier si et seulement si $s_{p-2} \equiv 0[M]$.

2. Donner une majoration de la complexité d'un test de primalité de M utilisant $(*)$ en fonction de la taille de M.

On pose $\omega = 2 + \sqrt{3}$ et $\overline{\omega} = 2 - \sqrt{3}$.

3. Vérifier que $s_k = \omega^{2^k} + \overline{\omega}^{2^k}$ pour tout $k \in \mathbb{N}$.

4. Supposons que $s_{p-2} \equiv 0[M]$. Soit $k \in \mathbb{N}$ tel que $s_{p-2} = kM$. Montrer que $\omega^{2^{p-1}} = kM\omega^{2^{p-2}} - 1$.

5. On suppose que M n'est pas premier et que $s_{p-2} \equiv 0[M]$. Soit q un facteur premier (impair) de M. Soit X l'anneau $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$. Si $x = (a, b) \in \mathbb{F}_q^2$, on note $x = a + b\sqrt{3}$ et on note $\mathbb{F}_q \oplus \mathbb{F}_q\sqrt{3}$ au lieu de $\mathbb{F}_q^2$.

a. Soit $\phi : X \to \mathbb{F}_q \oplus \mathbb{F}_q\sqrt{3}$ définie par

$$\phi(a + b\sqrt{3} + q\mathbb{Z}[\sqrt{3}]) = a[q] + b[q]\sqrt{3},$$

pour tous $a, b \in \mathbb{Z}$. Montrer que $\phi : (X, +) \to (\mathbb{F}_q \oplus \mathbb{F}_q\sqrt{3}, +)$ est un isomorphisme de groupes. Quel est le cardinal de X ?

Soit $\pi : \mathbb{Z}[\sqrt{3}] \twoheadrightarrow X$ la projection canonique.

b. Montrer que $\pi(\omega)$ est d'ordre 2^p dans $X^\times$.

c. Aboutir à une contradiction.

6. On suppose maintenant que M est premier.

a. Montrer que $\left(\frac{3}{M}\right) = -1$ (où $\left(\frac{\cdot}{\cdot}\right)$ désigne le symbole de Legendre).

b. Montrer que $\left(\frac{2}{M}\right) = 1$ (on pourra montrer directement que 2 est un carré modulo M en partant de $2^p \equiv 1[M]$).

Soient $X = \mathbb{Z}[\sqrt{3}]/M\mathbb{Z}[\sqrt{3}]$ et $\pi : \mathbb{Z}[\sqrt{3}] \twoheadrightarrow X$ la projection canonique. Soit $\sigma = 2\sqrt{3}$.

c. Montrer que $\pi\big((6 + \sigma)^M\big) = \pi(6 - \sigma)$.

d. Montrer que $\omega = \frac{(6+\sigma)^2}{24}$. Montrer que $\pi(\omega^{(M+1)/2}) = \pi(-1)$ (on pourra utiliser le fait que $24^{(M-1)/2} = (2^{(M-1)/2})^3.3^{(M-1)/2}$).

e. Conclure en multipliant chaque membre de l'égalité par $\overline{\omega}^{(M+1)/4}$.