Exercices et problèmes de cryptographie
Damien Vergnaud
Exercice complémentaire n° 6.8 (bis)

Le test de Lucas-Lehmer est un test de primalité pour les nombres de Mersenne, c'est-à-dire les nombres de la forme $M_p = 2^p - 1$ où p est un nombre premier.

Exercice 6.8 (bis) NOMBRES DE MERSENNE ET TEST DE LUCAS-LEHMER

1. Soit k un entier positif. Montrer que si l'entier $2^k - 1$ est un nombre premier alors k est un nombre premier.

Soit p un nombre premier et considérons la suite

$$s_i = \begin{cases} 4 & \text{si } i = 0 \\ s_{i-1}^2 - 2 & \text{sinon.} \end{cases}$$

Nous allons montrer que M_p est premier si et seulement si

$$s_{p-2} \equiv 0 \bmod M_p.$$

2. Posons $\omega = 2 + \sqrt{3}$ et $\bar{\omega} = 2 - \sqrt{3}$. Montrer par récurrence que

$$s_i = \omega^{2^i} + \bar{\omega}^{2^i} \tag{1}$$

pour tout entier $i \in \mathbb{N}$.

3. Dans cette question, nous supposons que $s_{p-2} \equiv 0 \bmod M_p$ et nous allons montrer que M_p est premier.
   (a) Montrer qu'il existe un entier $k \in \mathbb{N}$ tel que

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1$$

   (b) Supposons par l'absurde que M_p est premier et posons q le plus petit facteur premier de M_p (avec $1 < q < M_p$). Posons

$$A = \{a + b\sqrt{3}, a, b \in (\mathbb{Z}/q\mathbb{Z})\}.$$

   En considérant l'ordre de ω dans A, montrer que l'on obtient une contradiction.

4. Supposons réciproquement que M_p est premier.
   (a) Montrer que $2^{(M_p-1)/2} \equiv 1 \bmod M_p$ et $3^{(M_p-1)/2} \equiv -1 \bmod M_p$.
   (b) Considérons l'anneau

$$A' = \{a + b\sqrt{3}, a, b \in \mathbb{Z}_{M_p}\}.$$

   et l'élément $\sigma = 2\sqrt{3}$ de A'. Calculer $(6 + \sigma)^{M_p}$.
   (c) Montrer que $\omega = (6 + \sigma)^2/24$ et en déduire la valeur de $\omega^{(M_p+1)/2} = -1 \bmod M_p$.
   (d) En déduire que $s_{p-2} \equiv 0 \bmod M_p$

Solution :

1. Il suffit d'écrire la somme de la série géométrique :

$$1 + 2^a + (2^a)^2 + ... + (2^a)^{b-1} = \frac{2^{ab} - 1}{2^b - 1}$$

et si $k = ab$ avec $b > 1$, $2^b - 1$ est un diviseur propre de $2^k - 1$.

2. Pour $i = 0$, nous avons

$$\omega^{2^0} + \bar{\omega}^{2^0} = \omega + \bar{\omega} = 2 + \sqrt{3} + 2 - \sqrt{3} = 4 = s_0.$$

et la relation (1) est donc bien vérifiée pour $i = 0$. Supposons la satisfaite pour un entier $i \in \mathbb{N}$. Par la relation de récurrence, nous avons

$$\begin{aligned} s_{i+1} &= s_i^2 - 2 \\ &= (\omega^{2^i} + \bar{\omega}^{2^i})^2 - 2 \\ &= \omega^{2^{i+1}} + \bar{\omega}^{2^{i+1}} + 2(\omega\bar{\omega})^{2^i} - 2 \\ &= \omega^{2^{i+1}} + \bar{\omega}^{2^{i+1}} \end{aligned}$$

puisque $\omega\bar{\omega} = (2+\sqrt{3})(2-\sqrt{3}) = 4-3 = 1$. Par récurrence, nous avons donc montré que la relation (1) est vérifiée pour tout entier $i \in \mathbb{N}$.

3. (a) D'après la question précédente, il existe un entier $k \in \mathbb{N}$ tel que

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = kM_p.$$

En multipliant cette égalité par $\omega^{2^{p-2}}$, nous obtenons

$$(\omega^{2^{p-2}})^2 + (\omega\bar{\omega})^{2^{p-2}} = kM_p\omega^{2^{p-2}},$$

et comme $\omega\bar{\omega} = 1$, nous obtenons bien le résultat.

(b) L'ensemble A muni de l'addition et de la multiplication est un anneau. Le groupe multiplicatif A^* formé des éléments inversibles pour la multiplication est d'ordre au plus $q^2 - 1$ (car 0 n'est pas inversible). Dans cette anneau, nous avons $M_p \equiv 0 \bmod q$ et donc

$$\omega^{2^{p-1}} \equiv -1 \bmod q.$$

En mettant cette égalité au carré, nous avons $\omega^{2^p} \equiv 1 \bmod q$ et donc ω est inversible dans A (d'inverse ω^{2^p-1}). De plus, l'ordre de ω dans A^* est égal à 2^p (puisqu'il divise 2^p mais n'est pas égal à 2^{p-1}. L'ordre d'un élement de A^* est inférieur à l'ordre du groupe, donc nous avons

$$2^p \leq q^2 - 1 < q^2.$$

Mais puisque q est le plus petit facteur premier de M_p, nous avons $q^2 \leq M_p = 2^p - 1$ et nous obtenons la contradiction. Le nombre de Mersenne M_p est donc premier dès que $s_{p-2} \equiv 0 \bmod M_p$.

4. (a) L'entier 2 est un carré modulo M_p (puisque $2^p \equiv 1 \bmod M_p$ et donc $2 = 2^{p+1} = (2^{(p+1)/2})^2 \bmod M_p$) et par le critère d'Euler, nous avons

$$2^{(M_p-1)/2} \equiv 1 \bmod M_p.$$

Pour tout nombre premier p, $2^p - 1 \equiv 7 \bmod 12$, donc nous avons

$$\left(\frac{3}{M_p}\right) = -1$$

et par le critère d'Euler

$$3^{(M_p-1)/2} \equiv -1 \bmod M_p.$$

(b) En remarquant que $(x+y)^{M_p} \equiv x^{M_p} + y^{M_p}$ dans l'anneau A', nous avons

$$\begin{aligned}(6+\sigma)^{M_p} &= 6^{M_p} + (2^{M_p})(\sqrt{3}^{M_p}) \\ &= 6 + 2(3^{(M_p-1)/2})\sqrt{3} \\ &= 6 + 2(-1)\sqrt{3}\end{aligned}$$

donc $(6+\sigma)^{M_p} = 6 - \sigma$.

(c) Nous avons $(6+\sigma)^2 = 36 + 12 + 12\sigma = 48 + 12\sigma = 24\omega$. Par conséquent, nous obtenons

$$\begin{aligned}\omega^{(M_p+1)/2} &\equiv (6+\sigma)^{M_p+1}/24^{(M_p+1)/2} \\ &\equiv (6+\sigma)^{M_p}(6+\sigma)/(24 \times 24^{(M_p-1)/2}) \bmod M_p.\end{aligned}$$

Nous avons

$$24^{(M_p-1)/2} \equiv (2^{(M_p-1)/2})^3(3^{(M_p-1)/2}) \equiv (1)^3(-1) \equiv -1 \bmod M_p,$$

et donc finalement

$$\begin{aligned}\omega^{(M_p+1)/2} &\equiv (6-\sigma)(6+\sigma)/(-24) \\ &\equiv -1 \bmod M_p\end{aligned}$$

puisque $M_p \equiv 3 \bmod 4$.

(d) En multipliant l'égalité précédente par $\bar{\omega}^{(M_p+1)/4}$, nous obtenons

$$\omega^{(M_p+1)/2}\bar{\omega}^{(M_p+1)/4} = -\bar{\omega}^{(M_p+1)/4}$$

et puisque $\omega\bar{\omega} = 1$,

$$0 = \omega^{(M_p+1)/4} + \bar{\omega}^{(M_p+1)/4} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = s_{p-2}.$$

□