

Interrogation écrite n° 1

Il est demandé de faire clairement référence aux résultats vus en cours ou en TD. Tous les documents sont interdits.

Exercice 1. Soit $n \geq 2$ un entier naturel.

1. Montrer que n est premier si et seulement s'il existe un entier x d'ordre $n - 1$ dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.
2. Soit un groupe G noté multiplicativement, d'élément unité 1. Montrer qu'un élément $g \in G$ est d'ordre k si et seulement si $g^k = 1$ et si $g^{k/p} \neq 1$ pour tout diviseur premier p de k .
3. On suppose que, pour chaque diviseur p de $n - 1$, il existe un nombre x_p tel que :

$$x_p^{\frac{n-1}{p}} \pmod{n} \neq 1, \quad \text{et} \quad x_p^{n-1} \pmod{n} = 1.$$

Construire un élément d'ordre $n - 1$ et conclure que n est premier. *Indication* : soit λ_p l'ordre de x_p dans $(\mathbb{Z}/n\mathbb{Z})^*$; justifier l'existence un élément x d'ordre le plus petit multiple commun de la famille $\{\lambda_p, p|n\}$. Montrer que cet élément x est d'ordre $n - 1$.

Exercice 2. Soit f une fonction de chiffrement *RSA*, c'est-à-dire de la forme :

$$f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x^e,$$

avec $n = pq$. On identifie $\mathbb{Z}/n\mathbb{Z}$ avec $\{0, 1, \dots, n - 1\}$. On considère la fonction $\delta : \mathbb{Z}/n\mathbb{Z} \rightarrow \{0, 1\}$ définie ainsi :

$$\delta(y) = \begin{cases} 0, & \text{si } 0 \leq f^{-1}(y) < \frac{n}{2}, \\ 1, & \text{si } \frac{n}{2} \leq f^{-1}(y) \leq n - 1. \end{cases}$$

1. Montrer les équivalences :

$$\begin{aligned} \delta(f(x)) = 0 &\iff x \in \left[0, \frac{n}{2}\right[, \\ \delta(f(2x)) = 0 &\iff x \in \left[0, \frac{n}{4}\right[\cup \left[\frac{n}{2}, \frac{3n}{4}\right[. \end{aligned}$$

Généraliser à $\delta(f(2^i x))$. *Indication* : considérer l'écriture des nombres en base deux.

2. Montrer comment transformer tout algorithme polynomial calculant $\delta(y)$ pour tout y en un algorithme polynomial qui calcule $f^{-1}(y)$ pour tout y .
3. En déduire qu'il est aussi difficile de déterminer le premier bit d'un message en clair à partir du message chiffré par une fonction *RSA* que de déterminer le message en clair tout entier.

Exercice 3. Soit p et q deux entiers premiers distincts, tous les deux congrus à 3 modulo 4. Soit $n = pq$, et soit C un carré modulo n , c'est-à-dire $C = M^2 \pmod n$ pour un certain entier M modulo n . On considère la procédure suivante :

- (a) Trouver deux entiers h et k tels que $hp + kq = 1$.
- (b) Calculer modulo n :

$$x = hpb + kqa \pmod n, \quad y = hpb - qka \pmod n, \quad (1)$$

où on a posé

$$a = C^{\frac{p+1}{4}} \pmod p, \quad b = C^{\frac{q+1}{4}} \pmod q.$$

1. Montrer que, connaissant p , q et C , la procédure s'exécute en temps polynomial. Où utilise-t-on l'hypothèse $p = q = 3 \pmod 4$?
2. (a) Montrer qu'un entier α est une racine carrée de A modulo n si et seulement si α est une racine carrée de A modulo p et α est une racine carrée de A modulo q .
- (b) Montrer que si un entier z non congru à p est un carré modulo p , alors

$$z^{\frac{p-1}{2}} \pmod p = 1.$$

En déduire que pour tout entier z qui est un carré modulo p , on a

$$z^{\frac{p+1}{2}} \pmod p = z.$$

- (c) Montrer que les éléments x et y définis en (1) ci-dessus sont des racines carrées de C modulo n .
3. Montrer que les seules racines carrées de C modulo n sont parmi $\pm x, \pm y$.