

Interrogation écrite n° 1

Correction

Exercice 1.

1. Si n est premier alors on sait que $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique d'ordre $n-1$. Il existe donc un élément d'ordre $n-1$. Réciproquement, s'il existe un élément d'ordre $n-1$ dans $G = (\mathbb{Z}/n\mathbb{Z})^*$ alors comme G est d'ordre au plus $n-1$ il est en fait d'ordre $n-1$. Donc $\phi(n) = n-1$. Mais si n est composé, disons $n = ab$ avec a et b premiers entre eux et $a, b \neq 1$, alors $\phi(n) = \phi(a)\phi(b) \leq (a-1)(b-1) < n-1$, contradiction.
2. Si g est d'ordre k , il est clair que $g^k = 1$ et $g^{k/p} \neq 1$ puisque $k/p < k$. Réciproquement, supposons que $g^k = 1$ et $g^{k/p} \neq 1$ pour p diviseur premier de k . Alors l'ordre l de g divise k . Si $l \neq k$, alors $k = plf$ avec p premier et $f \geq 1$. Mais alors p divise k donc $g^{k/p} \neq 1$, ce qui contredit $g^l = 1$. Donc $l = k$.
3. On a vu que dans un groupe commutatif, si u et v sont les ordres d'éléments du groupe, il existe un élément d'ordre le ppcm de u et v . Par récurrence, ce résultat se généralise aux familles finies d'éléments. Ceci justifie l'existence d'un élément x d'ordre le ppcm des λ_p , où p parcourt les diviseurs premiers de $n-1$. Montrons que l'ordre λ de x est égal à $n-1$.

On a $\lambda_p | n-1$ puisque $x_p^{n-1} = 1 \pmod n$, et ceci pour tout diviseur premier $p | n-1$. Il s'ensuit que $\lambda | n-1$. Supposons que λ est un diviseur strict de $n-1$. Alors il existe un diviseur premier q de $n-1$ tel que $q\lambda_p | n-1$ pour tout diviseur premier p de $n-1$. En particulier pour $p = q$, on a $\lambda_q | \frac{n-1}{q}$, ce qui contredit $x_q^{\frac{n-1}{q}} \neq 1 \pmod n$. Donc $\lambda = n-1$. Il s'ensuit, d'après la question 1. ci-dessus, que n est premier.

Exercice 2.

1. On a :

$$\delta(f(2^i x)) = 0 \iff x \in \bigcup_{j=0}^{2^i-1} \left[\frac{2j}{2^{i+1}}n, \frac{2j+1}{2^{i+1}}n \right[.$$

En effet, $\delta(f(2^i x)) = 0$ si et seulement si $2^i x$ est dans l'intervalle $[0, \frac{n}{2}[$, c'est-à-dire si le $(i+1)^{\text{e}}$ bit de x dans son écriture en base deux, en partant des bits de poids le plus fort, est égal à 0. C'est bien l'union d'intervalles décrite ci-dessus.

2. Tout entier $x < n$ s'écrit en base deux avec un nombre de bits au plus égal à $N = \lfloor \log_2(n) \rfloor$ (partie entière). De plus, connaissant $y = f(x)$, on calcule $f(2x)$ par la multiplication $f(x) \times 2^e$, qui se fait en temps polynomial. On obtient de proche en proche le $(i+1)^{\text{e}}$ bit de $x = f^{-1}(y)$ en temps polynomial pour chaque i , en calculant $f(2^i x)$ comme le produit $f(2^{i-1} x) \times 2^e$, en appliquant l'algorithme δ à la valeur ainsi obtenue de $f(2^i x)$, et en utilisant la correspondance du 1. ci-dessus pour déterminer la valeur du bit. Tous les bits de x sont finalement déterminés en temps polynomial.
3. D'après la question précédente, la détermination de la parité du bit de tête de $x = f^{-1}(y)$ à partir de y fournit un algorithme permettant de reconstruire x tout entier.

Exercice 3.

1. Les entiers p et q sont premiers et distincts donc premiers entre eux. L'existence de h et k est donc assurée. L'algorithme d'Euclide étendu permet de trouver deux entiers h et k en temps polynomial. Connaissant p et q , le produit n puis le calcul de a et b par élévation rapide à la puissance modulo n , enfin les produits et sommes pour trouver x et y sont tous des opérations polynomiales en la taille des entrées.

On utilise $p = q = 3 \pmod 4$ pour définir a et b , puisqu'alors les puissances $\frac{p+1}{4}$ et $\frac{q+1}{4}$ sont entières.

2. (a) En effet pour tout entier X , on a $X = 0 \pmod n$ si et seulement si $X = 0 \pmod p$ et $X = 0 \pmod q$. On applique cette remarque à $\alpha^2 - A$, où A est le nombre hypothétique dont α est une racine carrée modulo n .
- (b) Si z est une racine carrée modulo p , écrivons $z = A^2 \pmod p$. Alors $A \not\equiv 0 \pmod p$ donc $A^{p-1} = 1 \pmod p$ d'après le théorème de Fermat ; d'où $z^{\frac{p-1}{2}} = 1 \pmod p$. La deuxième égalité s'en déduit, en remarquant qu'elle est encore vraie pour $z = 0 \pmod p$.
- (c) Vérifions que x est racine carrée de C modulo n . D'après ce qu'on a vu en 2a ci-dessus, il suffit de vérifier que $x^2 = C \pmod p$ et $x^2 = C \pmod q$. Calculons modulo p :

$$\begin{aligned} x^2 &= (hpb + kqa)^2 = (kq)^2 a^2 \\ &= (1 - hp)^2 a^2 = a^2 = C^{\frac{p+1}{2}} \\ &= C \pmod p \end{aligned} \qquad \text{d'après 2b.}$$

De même, on trouve $x^2 = C \pmod q$ et donc finalement $x^2 = C \pmod n$. De la même façon, on obtient que y est une racine carrée de C modulo n .

3. Il reste à montrer que $\pm x$ et $\pm y$ sont bien les *seules* racines carrées de C modulo n . D'après le théorème des restes chinois, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Si x est un entier modulo n représenté par le couple (u, v) dans l'anneau produit, les racines de x modulo n sont donc représentées dans l'anneau produit par les couples $(\pm u', \pm v')$, où u' et v' sont des racines de u et v modulo p et q respectivement. Les racines carrées de x^2 modulo n sont donc au nombre de :

- (a) Une, si $x = 0 \pmod n$;
 (b) Deux, si $x = 0 \pmod p$ et $x \neq 0 \pmod q$, ou si $x = 0 \pmod q$ et $x \neq 0 \pmod p$;
 (c) Quatre dans les autres cas.

Or on remarque si $x = y \pmod n$, alors $a = 0 \pmod p$ donc $C = 0 \pmod p$, c'est-à-dire $M = 0 \pmod p$. On est donc dans le cas (a) ou (b) ci-dessus de deux racines au plus. Si de plus $x = -x \pmod n$ alors $x = y = 0 \pmod n$, d'où on tire $b = 0 \pmod q$ donc $C = 0 \pmod q$ et finalement $C = 0 \pmod n$. Dans tous les cas il y a bien autant d'éléments dans $\{\pm x, \pm y\}$ que de racines carrées de $C = M^2 \pmod n$.