Exercices et problèmes de cryptographie
Damien Vergnaud
Exercice complémentaire n° 6.5 (bis)

Le but de cet exercice est de démontrer la loi de réciprocité quadratique (Théorème 6.3).

Exercice 6.5 (bis) LOI DE RÉCIPROCITÉ QUADRATIQUE

Soient p et q deux nombres premiers impairs distincts. Posons

$$\mathcal{A} = \{(k \bmod p, k \bmod q), k \in \{1, \ldots, (pq-1)/2\}, \mathrm{pgcd}(k, pq) = 1\},$$

et

$$\mathcal{B} = \{(i, j), i \in \{1, \ldots, p-1\}, j \in \{1, \ldots, (q-1)/2\}\},$$

et considérons les éléments $\pi_{\mathcal{A}} = \prod_{c \in \mathcal{A}} c$ et $\pi_{\mathcal{B}} = \prod_{c \in \mathcal{B}} c$ du groupe $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

1. Montrer que $\pi_{\mathcal{A}} = \left(\dfrac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}} \bmod p, \dfrac{(q-1)!^{(p-1)/2}}{p^{(q-1)/2}} \bmod q \right)$.
2. Montrer que $\pi_{\mathcal{B}} = \left((p-1)!^{(q-1)/2} \bmod p, (-1)^{(p-1)(q-1)/4}(q-1)!^{(p-1)/2} \bmod q\right)$
3. Montrer que $\mathcal{A}$ et $\mathcal{B}$ sont des systèmes de représentants des éléments du groupe $((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)/U$ où U est le sous groupe à deux éléments $\{(1,1), (-1,-1)\} \subset ((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)$.
4. En déduire que les éléments $\pi_{\mathcal{A}}$ et $\pi_{\mathcal{B}}$ sont égaux dans le groupe $((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)/U$ et la loi de réciprocité quadratique.

Solution :

1. Pour la première coordonnée de $\pi_{\mathcal{A}} = \prod_{c\in\mathcal{A}} c$, nous avons

$$\pi_{\mathcal{A}}^{(1)} = \frac{\left(\prod_{i=1}^{p-1} i\right)\cdot\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1}((q-1)/2-1)p+i\right)\left(\prod_{i=1}^{(p-1)/2} p\cdot(q-1)/2+i\right)}{q\cdot 2q\cdot 3q\cdots(p-1)/2q}$$

et donc

$$\pi_{\mathcal{A}}^{(1)} \equiv \frac{\left(\prod_{i=1}^{p-1} i\right)\cdot\left(\prod_{i=1}^{p-1} i\right)\cdots\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{(p-1)/2} i\right)}{q^{(p-1)/2}((p-1)/2)!} \bmod p$$

et

$$\pi_{\mathcal{A}}^{(1)} = \frac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}} \bmod p.$$

De même nous avons

$$\pi_{\mathcal{A}}^{(2)} = \frac{(q-1)!^{(p-1)/2}}{p^{(q-1)/2}} \bmod q.$$

2. Pour la première coordonnée de $\pi_{\mathcal{B}} = \prod_{c\in\mathcal{B}} c$, nous avons

$$\pi_{\mathcal{B}}^{(1)} = \prod_{j\in\{1,\ldots,(q-1)/2\}}\ \prod_{i\in\{1,\ldots,p-1\}} i = (p-1)!^{(q-1)/2}$$

et pour la seconde coordonnée de $\pi_{\mathcal{B}}$, nous avons

$$\pi_{\mathcal{B}}^{(2)} = \prod_{i\in\{1,\ldots,p-1\}}\ \prod_{j\in\{1,\ldots,(q-1)/2\}} j = ((q-1)/2)!^{(p-1)}.$$

Or nous avons

$$\begin{aligned}(q-1)! &= \left(\prod_{k=1}^{(q-1)/2} k\right)\cdot\left(\prod_{k=(q-1)/2+1}^{(q-1)} k\right)\\ &= \left(\prod_{k=1}^{(q-1)/2} k\right)\cdot(-1)^{(q-1)/2}\left(\prod_{k=(q-1)/2+1}^{(q-1)}(q-k)\right)\\ &= (-1)^{(q-1)/2}\left(\prod_{k=1}^{(q-1)/2} k\right)^2\end{aligned}$$

et donc

$$((q-1)/2)!^2 = (-1)^{(q-1)/2}(q-1)!.$$

Finalement, nous obtenons

$$\pi_{\mathcal{B}}^{(2)} = (-1)^{(p-1)(q-1)/4}(q-1)!^{(p-1)/2}.$$

3. Nous allons montrer que $\mathcal{A}$ et $\mathcal{B}$ sont des systèmes de représentants des éléments du groupe $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)/U$ où U est le sous groupe à deux éléments $\{(1,1),(-1,-1)\}\subset((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)$. Il s'agit du groupe $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)$ où les éléments (a,b) et $(-a \bmod p, -b \bmod q)$ sont identifiés. Le fait que $\mathcal{B}$ est un système de représentants est immédiat (il est de cardinal $(p-1)(q-1)/2$ et les éléments sont deux à deux distincts pour cette relation d'équivalence). Par le théorème chinois des restes, nous obtenons également que $\mathcal{A}$ est un système de représentants de $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)/U$. En effet, le groupe $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)$ est isomorphe à $(\mathbb{Z}/pq\mathbb{Z})^*$ par l'application

$$\begin{array}{ccc}(\mathbb{Z}/pq\mathbb{Z})^* & \longrightarrow & ((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)\\ k & \longmapsto & (k \bmod p, k \bmod q)\end{array}$$

et donc le groupe $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)/U$ est isomorphe à $(\mathbb{Z}/pq\mathbb{Z})^*/\{-1,1\}$ par la même application. Comme $\{k\in\{1,\ldots,(pq-1)/2\}, \text{pgcd}k,pq=1\}$ est un système de représentants de $(\mathbb{Z}/pq\mathbb{Z})^*/\{-1,1\}$, $\mathcal{A}$ est un système de représentants de $((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)/U$.

4. Les éléments $\pi_{\mathcal{A}}$ et $\pi_{\mathcal{B}}$ sont donc égaux dans le groupe $((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)/U$, et dans nous avons donc

$$\pi_{\mathcal{A}} = \pi_{\mathcal{B}} \text{ ou } \pi_{\mathcal{A}} = (-1,-1) \cdot \pi_{\mathcal{B}}$$

dans le groupe $((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)$. Dans les deux cas, nous en déduisons :

$$\pi_{\mathcal{A}}^{(1)} \cdot \pi_{\mathcal{A}}^{(2)} = \pi_{\mathcal{B}}^{(1)} \cdot \pi_{\mathcal{B}}^{(2)},$$

soit

$$\frac{(p-1)!^{(q-1)/2}}{q^{(p-1)/2}} \cdot \frac{(q-1)!^{(p-1)/2}}{p^{(q-1)/2}} = (p-1)!^{(q-1)/2} \cdot (-1)^{(p-1)(q-1)/4} (q-1)!^{(p-1)/2}$$

d'où

$$p^{(q-1)/2} \cdot q^{(p-1)/2} = (-1)^{(p-1)(q-1)/4}$$

et par le critère d'Euler (Théorème 6.2)

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

□