Université Paris Diderot — MI4– Année 2009/10
Département de Sciences Exactes — L2 Info

Examen du 24 juin 2010 (deuxième session)

Les exercices sont indépendants. Les documents autorisés sont le polycopié, les notes de cours et TD. Les calculatrices ne sont pas autorisées. On rappelle que $\phi(n)$ désigne l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et $\lambda(n)$ désigne l'ordre maximal d'un élément de ce groupe.

Exercice 1 Résoudre en nombres entiers chacune des équations suivantes

$$1389x + 177y = 4 \tag{1}$$

$$1389x + 177y = 6 \tag{2}$$

Exercice 2 Résoudre en nombres entiers les systèmes d'équations suivants

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 3 \mod 91 \end{cases} \tag{3}$$

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 15 \mod 91 \end{cases} \tag{4}$$

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 15 \mod 91 \\ x \equiv 10 \mod 16 \end{cases} \tag{5}$$

Exercice 3 Si N est un nombre impair, on décompose $N - 1 = 2^s M$ avec M impair et on pose

$$S := \left\{ a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^M = 1 \text{ ou } \exists r \in [0, s-1],\ a^{2^r M} = -1 \right\}.$$

1. Calculer le cardinal de S pour $N = 83$.
2. Soit $L \geq 1$, combien de solutions modulo 97 possède l'équation $a^L \equiv 1 \mod 97$?
3. Combien de solutions modulo 83 possède l'équation $a^2 \equiv 1 \mod 83$ (resp. $a^4 \equiv 1 \mod 83$) ?
4. Calculer le cardinal de S pour $N = 8051 = 83.97$.

Exercice 4 Soit $L := 656 = 2^4.41$, $M := 561 = 3.11.17$.

1. Calculer $\phi(L)$ et $\phi(M)$.
2. Calculer $\lambda(L)$ et $\lambda(M)$.
3. Les groupes $(\mathbb{Z}/656\mathbb{Z})^*$, $(\mathbb{Z}/561\mathbb{Z})^*$ sont-ils isomorphes ?

Exercice 5 *On suppose que $N = pq$ est le produit de deux premiers distincts, que c est le paramètre pour coder, i.e. on transforme un message m en $m' = m^c \mod N$ avant de l'envoyer. On note d l'inverse de $c \mod \phi(N)$, de sorte que le décodage s'effectue en calculant $m = m'^d \mod N$. Dans le système RSA les paramètres (N, c) sont publics, le paramètre d est secret.*

1. Soit $N = 35$ et $c = 11$. Coder le message $m = 2$ et vérifiez le résultat en le décodant.
2. Vos paramètres publics sont $(N, c) = (581, 211)$, vous savez que $581 = 7.83$ et vous recevez le message $m' = 3$. Quel est le message original qui vous a été envoyé ?