Université Paris Diderot — MI4– Année 2010/11
Département de Sciences Exactes — L2 Info

Examen du 20 mai 2011 :

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

$$1539x + 585y = 18 \tag{1}$$

$$1539x + 585y = 15 \tag{2}$$

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

$$\begin{cases} x \equiv 2 \mod 117 \\ x \equiv 5 \mod 36 \end{cases} \tag{3}$$

$$\begin{cases} x \equiv 2 \mod 117 \\ x \equiv 11 \mod 36 \end{cases} \tag{4}$$

$$\begin{cases} x \equiv 2 \mod 117 \\ x \equiv 11 \mod 36 \\ x \equiv 4 \mod 5 \end{cases} \tag{5}$$

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 $N = 59$.
2. Soit $L \geq 1$, combien de solutions modulo 59 possède l'équation $a^L \equiv 1 \mod 59$?
3. Combien de solutions modulo 17 possède l'équation $a^2 \equiv -1 \mod 17$ (resp. $a^4 \equiv -1 \mod 17$) ?
4. Calculer le cardinal de S pour $N = 1003 = 17.59$.

Exercice 4 Soit $L := 225 = 3^2.5^2$, $M := 143 = 11.13$ et $N := 248 = 2^3.31$.

1. Calculer $\phi(L)$, $\phi(M)$ et $\phi(N)$.
2. Calculer $\lambda(L)$, $\lambda(M)$ et $\lambda(N)$.
3. Montrer que les groupes $(\mathbb{Z}/225\mathbb{Z})^*$ et $(\mathbb{Z}/143\mathbb{Z})^*$ sont isomorphes. Les groupes $(\mathbb{Z}/225\mathbb{Z})^*$ et $(\mathbb{Z}/248\mathbb{Z})^*$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 $N = 55$ et $c = 7$. Coder le message $m = 2$ et vérifiez le résultat en le décodant.
2. Vos paramètres publics sont $(N, c) = (649, 83)$, vous savez que $649 = 11.59$ et vous recevez le message $m' = 3$. Quel est le message original qui vous a été envoyé ?