Université Paris Diderot
Département de Sciences Exactes

MI4– Année 2011/12
L2 Info

Examen du 25 mai 2012 :

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

$$3381x + 875y = 8 \tag{1}$$

$$3381x + 875y = 7. \tag{2}$$

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

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 4 \mod 55 \end{cases} \tag{3}$$

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 6 \mod 55 \end{cases} \tag{4}$$

$$\begin{cases} x \equiv 1 \mod 35 \\ x \equiv 6 \mod 55 \\ x \equiv 3 \mod 6 \end{cases} \tag{5}$$

Exercice 3 Si N est un nombre impair, on décompose $N-1 = 2^s M$ avec M impair et on pose $R := \left\{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^{N-1} = 1\right\}$ et

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

1. Calculer le cardinal de R et de S pour $N = 29$.
2. Soit $L \geq 1$, combien de solutions modulo 29 possède l'équation $a^L \equiv 1 \mod 29$?
3. Combien de solutions modulo 13 possède l'équation $a^2 \equiv 1 \mod 13$ (resp. $a^2 \equiv -1 \mod 13$, resp. $a^4 \equiv -1 \mod 13$) ?
4. Calculer le cardinal de R et S pour $N = 377 = 13.29$.

Exercice 4 Soit $L := 700 = 2^2.7.5^2$, $M := 572 = 2^2.11.13$ et $N := 369 = 3^2.41$.

1. Calculer $\phi(L)$, $\phi(M)$ et $\phi(N)$.
2. Calculer $\lambda(L)$, $\lambda(M)$ et $\lambda(N)$.
3. Le groupe $(\mathbb{Z}/L\mathbb{Z})^*$ est-il cyclique ?
4. Montrer que les groupes $(\mathbb{Z}/700\mathbb{Z})^*$ et $(\mathbb{Z}/572\mathbb{Z})^*$ sont isomorphes. Les groupes $(\mathbb{Z}/700\mathbb{Z})^*$ et $(\mathbb{Z}/369\mathbb{Z})^*$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 $N = 65$ et $c = 7$. Coder le message $m = 2$ et vérifier le résultat en le décodant.
2. Vos paramètres publics sont $(N, c) = (533, 37)$, vous savez que $533 = 13.41$ et vous recevez le message $m' = 2$. Quel est le message original qui vous a été envoyé ?