TS Spé Pour le 9 juillet 2012

DM2 – Codage

1. On considère l'équation (E): $109x - 226y = 1$, où x, y sont des entiers relatifs.

(a) Déterminer le pgcd de 109 et 226. Que peut-on en déduire pour l'équation (E) ?

(b) Montrer que l'ensemble des solutions de (E) est l'ensemble des couples $(141 + 226\,k\,; 68 + 109\,k)$ où k appartient à $\mathbb{Z}$.

(c) En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel e tels que $109d = 1 + 226e$. *On précisera les valeurs des entiers e et d.*

2. Montrer que 227 est un nombre premier.

3. On note A l'ensemble des 227 entiers naturels a tels que $a \leq 226$. On considère deux fonctions f et g de A dans A définies ainsi :

- à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227 ;
- à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

(a) Vérifier que $g\big(f(0)\big) = 0$.

(b) Montrer que pour tout entier non nul a de A, $a^{226} \equiv 1\ [227]$.

(c) En utilisant **1.b.** déduire que quel que soit l'entier non nul a de A, $g\big(f(a)\big) = a$.

Application au codage

A tout entier x de l'ensemble A, on peut associer l'entier $f(x)$, la fonction f servant à coder et la fonction g à décoder puisque $g\big(f(x)\big) = x$. Comme on travaille modulo 227, on peut utiliser la correspondance Ascii qui va de 1 à 127. Comme certaines valeurs de $f(x)$ n'ont pas de correspondance dans la table Ascii, on laissera le message codé sous forme de nombre.

1. A l'aide d'un algorithme permettant de calculer les grandes puissances modulaires, coder le message suivant :

Message	O	U	I
Valeur de $x = code\ Ascii$			
Valeur de $f(x)$			

2. Décoder le message $63 - 177 - 63$.

Complément optionnel : Automatiser le codage et le décodage en utilisant un tableur ou un algorithme (et envoyer le fichier par mail à cqueru@afvalpo.cl)