Devoir n° 1

À rendre la semaine du 25 avril 2011

Exercice 1. *Équations en entiers naturels.*

1. Peut-on trouver des ***entiers naturels*** x et y tels que $7x + 11y = 60$?
   Même question pour l'équation $7x + 11y = 59$ [*indication : on pourra montrer que si* (x, y) *est un couple d'entiers naturels solution de l'équation* $7x + 11y = 59$*, alors* y *est compris entre* 0 *et* 5].

2. Dans toute cette question, a et b sont deux entiers naturels non nuls et premiers entre eux. Pour tout entier relatif c fixé, on considère l'équation

$$ax + by = c \ , \quad (x, y) \in \mathbb{Z}^2 \tag{1}$$

   (a) Montrer que quel que soit l'entier c, l'équation (1) admet des solutions dans $\mathbb{Z}^2$.
   (b) Montrer que si le couple (x, y) est solution de (1), alors pour tout $k \in \mathbb{Z}$, le couple $(x+kb, y-ka)$ est également solution. En déduire que pour tout entier c, l'équation (1) admet une solution $(x, y) \in \mathbb{Z}^2$ avec $0 \leq y \leq a - 1$.
   (c) En déduire que si $c > ab - a - b$, il existe (au moins) un couple (x, y) d'entiers positifs ou nuls solution de l'équation (1).
   (d) Montrer à l'inverse que si $c = ab - a - b$, il n'existe *aucun* couple (x, y) d'entiers positifs ou nuls solution de l'équation (1).

Exercice 2. *Attaque du chiffre de Hill.*

1. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice à coefficients dans $\mathbb{Z}/26\mathbb{Z}$. On pose $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Que vaut le produit AB ? En déduire que la matrice A est inversible si et seulement si $ad - bc$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$, et expliciter l'inverse de A le cas échéant.

2. Vous avez intercepté le message suivant de vos ennemis :

   YKTZZUDCLWQOAGKIHXRVANYSPWBYDCLS.

   Votre espion vous a informé que pour communiquer, l'état-major adverse utilise le chiffrement de Hill, avec une longueur de bloc m égale à 2. En outre, connaissant le protocole en vigueur dans les communications militaires, vous savez que ce message commence par "MONGENERAL". On note $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice de chiffrement.

   (a) Justifier que

$$\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix} = A \begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}. \tag{2}$$

   (b) Que suffirait-il pour retrouver A à partir de l'équation (2) ? Pourquoi est-ce impossible ici ?
   (c) Retrouver A en exploitant une autre égalité du même type que (2).
   (d) Décrypter le message complet.