Corrigé du devoir n° 1

Exercice 1. *Équations en entiers naturels.*

1. On remarque que $7 \times 7 + 11 \times 1 = 60$: il existe donc bien au moins une - c'est en fait la seule - solution en entiers naturels pour l'équation $7x + 11y = 60$.

   Il n'en va pas de même de l'équation $7x + 11y = 59$: si (x, y) est un couple d'entiers naturels solution de cette équation on a en particulier

   $$0 \leq 11y = 59 - 7x \leq 59$$

   d'où l'on déduit que y est compris entre 0 et 5 (quotient de la division euclidienne de 59 par 11). Il reste à tester ces 6 valeurs possibles pour y : si $y = 0$, alors $7x = 59$, ce qui est absurde car 59 n'est pas divisible par 7. De même, si $y = 1$ alors $7x = 48$ et 48 n'est pas divisible par 7, si $y = 2$ alors $7x = 37$ et 37 n'est pas divisible par 7, si $y = 3$ alors $7x = 26$ et 26 n'est pas divisible par 7, si $y = 4$ alors $7x = 15$ et 15 n'est pas divisible par 7, et enfin si $y = 5$ alors $7x = 4$ et 4 n'est pas divisible par 7. Il n'y a donc pas de solution en entiers naturels.

2. (a) Puisque a et b sont premiers entre eux, il existe deux entiers u et v tels que $au + bv = 1$. Si c est un entier quelconque, le couple $(x, y) = (uc, vc)$ est alors solution de l'équation $ax + by = c$.

   (b) Si $ax + by = c$, alors pour tout $k \in \mathbb{Z}$ on a $a(x + kb) + b(y - ka) = ax + by = c$. Soit q le quotient de la division euclidienne de y par a. Alors $y - qa = r$ est le reste de cette division, de sorte que l'on a $0 \leq r \leq a - 1$. Ainsi, le couple $(x', y') = (x + qb, y - qa)$ est une solution de l'équation initiale vérifiant $0 \leq y' \leq a - 1$.

   (c) Soit (x, y) une solution de l'équation $ax + by = c$ vérifiant $0 \leq y \leq a - 1$ (un tel couple existe d'après la question précédente). On a alors $ax = c - by > ab - a - b - b(a - 1) = -a$, d'où $x > -1$. Or x est un entier (relatif), donc la dernière inégalité équivaut à $x \geq 0$. On a donc bien trouvé un couple (x, y) d'entiers positifs ou nuls solution de l'équation $ax + by = c$.

   (d) Supposons par l'absurde que (x, y) soit un couple d'entiers positifs ou nuls solution de l'équation

   $$ax + by = ab - a - b.$$

   On a alors

   $$a(x + 1) = b(a - y - 1) \tag{1}$$

   et en particulier, b divise $a(x + 1)$. Comme a et b sont premiers entre eux, on en déduit (théorème de Gauss) que b divise $x + 1$. Comme x est un entier positif ou nul, il suit que $x + 1$ est un entier *strictement positif* divisible par b. En particulier $x + 1$ est supérieur ou égal à b, d'où, en reportant dans (1)

   $$ab \leq a(x + 1) = b(a - y - 1) = ab - b(y + 1) < ab$$

   ce qui est absurde.

Exercice 2. *Attaque du chiffre de Hill.*

1. On trouve $AB = \begin{pmatrix} ab - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \delta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ où l'on a posé $\delta = \det A := ad - bc$. Si δ est inversible dans $\mathbb{Z}/26\mathbb{Z}$, d'inverse δ', alors la matrice $A' = \delta' B$ vérifie

   $$AA' = A'A = \delta\delta' \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et A est donc bien inversible. Inversement, si A est inversible, on a $AC = CA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ pour une certaine matrice C, moyennant quoi $\det A \det C = 1$ (multiplicativité du déterminant), et $\det$ A est inversible dans $\mathbb{Z}/26\mathbb{Z}$.

2. (a) Puisque le message en clair commence par "MONGENERAL", ses 3 premiers blocs sont "MO", "NG" et "EN", ce qui donne, en codant chaque lettre par le nombre correspondant entre 0 et 26, les blocs (12 14), (13 6) et (4 13). Les blocs correspondants dans le message chiffré sont "YK", "TZ" et "ZU", soit (24 10), (19 25) et (25 20). La traduction matricielle de l'application du chiffre de Hill, qui applique chacun des 3 blocs "clairs" sur le bloc "chiffré" correspondant est

$$A\begin{pmatrix} 12 \\ 14 \end{pmatrix} = \begin{pmatrix} 24 \\ 10 \end{pmatrix} \quad , \quad A\begin{pmatrix} 13 \\ 6 \end{pmatrix} = \begin{pmatrix} 19 \\ 25 \end{pmatrix} \quad \text{et} \quad A\begin{pmatrix} 4 \\ 13 \end{pmatrix} = \begin{pmatrix} 25 \\ 20 \end{pmatrix}.$$

En regroupant les deux premières équations, on obtient donc l'égalité

$$\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix} = A\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix}.$$

(b) Pour retrouver A à partir de l'équation précédente, il suffirait que la matrice $\begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}$ soit inversible, auquel cas on pourrait écrire :

$$A = \begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix}\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix}^{-1}.$$

Malheureusement, la matrice $\begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}$ n'est pas inversible, car son déterminant $12\times 6 - 14\times 13 = 20$ n'est pas inversible dans $\mathbb{Z}/26\mathbb{Z}$ ...

(c) On peut en revanche exploiter la transformation des deuxième et troisième blocs pour obtenir l'équation matricielle

$$\begin{pmatrix} 19 & 25 \\ 25 & 20 \end{pmatrix} = A\begin{pmatrix} 13 & 6 \\ 4 & 13 \end{pmatrix}.$$

Cette fois-ci, la matrice $\begin{pmatrix} 13 & 6 \\ 4 & 13 \end{pmatrix}$ est bien inversible, car son déterminant $13\times 13 - 6\times 4 = 15$ est inversible dans $\mathbb{Z}/26\mathbb{Z}$. En utilisant la formule obtenue à la première question, on calcule son inverse qui vaut

$$7\begin{pmatrix} 13 & -6 \\ -4 & 13 \end{pmatrix} = \begin{pmatrix} 7\times 13 & -7\times 6 \\ -7\times 4 & 7\times 13 \end{pmatrix} = \begin{pmatrix} 13 & 24 \\ 10 & 13 \end{pmatrix}.$$

On obtient alors

$$A = \begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix}\begin{pmatrix} 13 & 24 \\ 10 & 13 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}.$$

(d) Pour décrypter le message complet, il suffit alors de calculer la matrice A^{-1} et de l'appliquer au message crypté : on trouve $A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ et le message en clair :

"MONGENERALSOUSMARINENNEMIREPEREZ"

(le Z n'est pas une faute d'orthographe,mais un moyen de compléter le message pour qu'il y ait un nombre pair de lettres !).