# Correction contrôle de mathématiques
## du mardi 18 décembre 2012

## Exercice 1

**ROC** **3 points**

1) cf cours
2) Soit $D = \text{pgcd}(a, b)$ et $d = \text{pgcd}(a - b, b)$
   - $D$ divise $a$ et $b$ donc divise $a - b$. $D$ divise donc $a - b$ et $a$. $D \leqslant d$ (1)
   - $d$ divise $a - b$ et $b$ donc divise $(a - b) + b = a$. $d$ divise donc $a$ et $b$. $d \leqslant D$ (2)

   De (1) et (2) on a : $D = d$.

## Exercice 2

**Application du cours** **5 points**

1) Par l'algorithme d'Euclide, on a :

$$\begin{aligned}
1386 &= 546 \times 2 + 294\\
546 &= 294 \times 1 + 252\\
294 &= 252 \times 1 + 42\\
252 &= 42 \times 6
\end{aligned}$$

Donc $\text{pgcd}(1386, 546) = 42$ et donc $\text{ppcm}(1386, 546) = \dfrac{1386 \times 546}{42} = 18\,018$

2) Par l'algorithme d'Euclide, on a :

$$\begin{aligned}
2013 &= 734 \times 2 + 545\\
734 &= 545 \times 1 + 189\\
545 &= 189 \times 2 + 167\\
189 &= 167 \times 1 + 22\\
167 &= 22 \times 7 + 13\\
22 &= 13 \times 1 + 9\\
13 &= 9 \times 1 + 4\\
9 &= 4 \times 2 + 1
\end{aligned}$$

Donc $\text{pgcd}(2013, 734) = 1$. Les nombres 2013 et 734 sont donc premiers entre eux.

3) On a : $5(14n + 3) + (-14)(5n + 1) = 70n + 15 - 70n - 14 = 1$

Il existe un couple $(u, v)$ tel que : $u(14n + 3) + v(5n + 1) = 1$, donc d'après le théorème de Bezout, les nombres $(14 + 3)$ et $(5n + 1)$ sont premiers entre eux.

$87 = 14 \times 6 + 3$ et $31 = 5 \times 6 + 1$ donc les nombres 87 et 31 sont respectivement de la forme $(14n + 3)$ et $(5n + 1)$. On a donc $\text{pgcd}(87, 31) = 1$

4) Soit $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$. on a donc les relations :

$$a = da' \quad \text{et} \quad b = db' \quad \text{avec} \quad \text{pgcd}(a', b') = 1 \quad \text{et} \quad m = da'b'$$

on a alors : $6a'b' = 102$ soit $a'b' = 17$

La seule décomposition de 17 est $1 \times 17$. Comme $a < b$, on a : $a' = 1$ et $b' = 17$. On en déduit alors que : $a = 6 \times 1 = 6$ et $b = 17 \times 6 = 102$

## Exercice 3

**BAC** **4 points**

1) On a : $269 = 13 \times 18 + 5$ et $239 = 17 \times 14 + 1$. Donc 239 vérifie le système.

2) $N \equiv 5 \pmod{13}$ donc il existe $y \in \mathbb{Z}$ tel que $N = 5 + 13y$
$N \equiv 1 \pmod{17}$ donc il existe $x \in \mathbb{Z}$ tel que $N = 1 + 17x$
On a donc : $N = 1 + 17x = 5 + 13y$

3) Résolution de : $17x - 13y = 4 \quad (1)$

- (1,1) est solution de (1) car : $17 \times 1 + 13 \times 1 = 4$
- soit $(x, y)$ une solution de (1), on a donc le système suivant :

$$\begin{cases} 17x - 13y = 4 \\ 17 \times 1 - 13 \times 1 = 4 \end{cases}$$

En soustrayant termes à termes, on obtient : $17(x - 1) - 13(y - 1) = 0$ soit $17(x - 1) = 13(y - 1) \quad (2)$.

13 divise $17(x - 1)$ et $\text{pgcd}(17, 13) = 1$, d'après le théorème de Gauss, il existe $k \in \mathbb{Z}$ tel que : $x - 1 = 13k$

En remplaçant dans (2), on obtient alors : $y - 1 = 17k$

Les solutions $(x, y)$ de l'équation sont de la forme :

$$\begin{cases} x = 1 + 13k \\ y = 1 + 17k \end{cases} \quad k \in \mathbb{Z}$$

4) On a : $1 + 17x = 5 + 13y \quad \Leftrightarrow \quad 17x - 13y = 4$. $x$ et $y$ vérifient donc les relations de la question précédente, donc $x = 1 + 13k$

En remplaçant : $N = 1 + 17x = 1 + 17(1 + 13k) = 1 + 17 + 221k = 18 + 221k$

## Exercice 4

**Le chiffrement de Hill** **8 points**

**Partie A Inverse de 23 modulo 26**

1) On a : $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$. Donc le couple $(-9, -8)$ est solution de $(E)$

2) Soit $(x, y)$ une solution de $(E)$, on a donc le système suivant :

$$\begin{cases} 23x - 26y = 1 \\ 23 \times (-9) - 26 \times (-8) = 1 \end{cases}$$

En soustrayant termes à termes, on obtient : $23(x+9) - 26(y+8) = 0$ soit $23(x+9) = 26(y+8) \quad (E2)$.

26 divise $23(x+9)$ et $\text{pgcd}(23, 26) = 1$, d'après le théorème de Gauss, il existe $k \in \mathbb{Z}$ tel que : $x + 9 = 26k$

En remplaçant dans $(E2)$, on obtient alors : $y + 8 = 23k$

Les solutions $(x, y)$ de l'équation $(E)$ sont de la forme :

$$\begin{cases} x = -9 + 26k \\ y = -8 + 23k \end{cases} \quad k \in \mathbb{Z}$$

3) Si $23a \equiv 1 \pmod{26}$, alors il existe $b \in \mathbb{Z}$ tel que : $23a = 1 + 26b$ donc $23a - 26b = 1$

$(a, b)$ est donc solution de $(E)$. $a$ est donc de la forme : $a = -9 + 26k \quad k \in \mathbb{Z}$. Si l'on veut $0 \leqslant a \leqslant 25$ il faut donc prendre $k = 1$ ce qui donne $a = -9 + 26 = 17$.

## Partie B Chiffrement de Hill

⚠ Dans toute cette partie les congruences sont toutes modulo 26.

1) On a la chaîne suivante :

$$\text{ST} \Rightarrow (18, 19) \Rightarrow (21, 20) \Rightarrow \text{VU}$$

Détails :
- $y_1 \equiv 11 \times 18 + 3 \times 19 \equiv 255$ or $255 = 26 \times 9 + 21$ donc $y_1 \equiv 21$
- $y_2 \equiv 7 \times 18 + 4 \times 19 \equiv 202$ or $202 = 26 \times 7 + 20$ donc $y_2 \equiv 20$

a) A l'aide l'algorithme, on trouve alors :

$$\begin{aligned} \text{PALACE} &\Rightarrow \text{PA} ;\ \text{LA} ;\ \text{CE} \\ &\Rightarrow (15,0) ;\ (11,0) ;\ (2;4) \\ &\Rightarrow (9,1) ;\ (17,25) ;\ (8,4) \\ &\Rightarrow \text{JB} ;\ \text{RZ} ;\ \text{IE} \\ &\Rightarrow \text{JBRZIE} \end{aligned} \qquad \begin{aligned} \text{RAPACE} &\Rightarrow \text{RA} ;\ \text{PA} ;\ \text{CE} \\ &\Rightarrow (17,0) ;\ (15,0) ;\ (2;4) \\ &\Rightarrow (5,15) ;\ (9,1) ;\ (8,4) \\ &\Rightarrow \text{FP} ;\ \text{JB} ;\ \text{IE} \\ &\Rightarrow \text{FPJBIE} \end{aligned}$$

b) Une même lettre n'est pas nécessairement codée de la même façon. En effet le A de PA est codé par B tandis que le A de RA est codé par P. Pour qu'une même lettre soit codée de la même façon, il faut que le couple qu'elle compose avec une autre lettre soit identique.

2) a) Si $(x_1 ; x_2)$ vérifie $(S_1)$ alors : $\begin{cases} 11x_1 + 3x_2 \equiv y_1 & (1) \\ 7x_1 + 4x_2 \equiv y_2 & (2) \end{cases}$

En faisant $4 \times (1) - 3 \times (2)$, on obtient :

$$\begin{array}{r}44x_1 + 12x_2 \equiv 4y_1\\ -21x_1 - 12x_2 \equiv -3y_2\\ \hline 23x_1 + 0x_2 \equiv 4y_1 - 3y_2\end{array}$$

or $-3 = -26 + 23$ donc $-3 \equiv 23$

on a donc : $23x_1 \equiv 4y_1 + 23y_2$

En faisant $-7 \times (1) + 11 \times (2)$, on obtient :

$$\begin{array}{r}-77x_1 - 21x_2 \equiv -7y_1\\ 77x_1 + 44x_2 \equiv 11y_2\\ \hline 0x_1 + 23x_2 \equiv -7y_1 + 11y_2\end{array}$$

or $-7 = -26 + 19$ donc $-7 \equiv 19$

on a donc : $23x_2 \equiv 19y_1 + 11y_2$

b) De la question A3), on a : $23a \equiv 1 \quad \Leftrightarrow \quad a \equiv 17$ Alors :

- $23x_1 \equiv 4y_1 + 23y_2 \quad \Leftrightarrow \quad x_1 \equiv 17(4y_1 + 23y_2)$

  $x_1 \equiv 68y_1 + 391y_2$ or $68 \equiv 16$ et $391 \equiv 1$ donc : $x_1 \equiv 16y_1 + y_2$
- $23x_2 \equiv 19y_1 + 11y_2 \quad \Leftrightarrow \quad x_2 \equiv 17(19y_1 + 11y_2)$

  $x_2 \equiv 323y_1 + 187y_2$ or $323 \equiv 11$ et $187 \equiv 5$ donc : $x_2 \equiv 11y_1 + 5y_2$

c) Inversement si $(x_1, x_2)$ vérifient $(S_3)$ alors :

- $11x_1 + 3x_2 \equiv 11(16y_1 + y_2) + 3(11y_1 + 5y_2) \equiv 176y_1 + 11y_2 + 33y_1 + 15y_2 \equiv 209y_1 + 26y_2$

  or $209 \equiv 1$ et $26 \equiv 0$ donc : $11x_1 + 3x_2 \equiv y_1$
- $7x_1 + 4x_2 \equiv 7(16y_1 + y_2) + 4(11y_1 + 5y_2) \equiv 112y_1 + 7y_2 + 44y_1 + 20y_2 \equiv 156y_1 + 27y_2$

  or $156 \equiv 0$ et $27 \equiv 1$ donc : $7x_1 + 4x_2 \equiv y_2$

$(x_1, x_2)$ vérifie bien $(S_1)$

d) On trouve l'algorithme suivant :

```
Variables
X, Y, Z, T
Initialisation
Lire X, Y
traitement
16 * X + Y → Z
11 * X + 5 * Y → T
Z − E (Z/26) * 26 → Z
T − E (T/26) * 26 → T
Sortie
Afficher Z, T
```

e) On obtient donc pour $PFXXKNUW$

$$\begin{aligned}\text{PFXXKNUW} &\Rightarrow \text{PF} ;\ \text{XX} ;\ \text{KN} ;\ \text{UW}\\ &\Rightarrow (15,5) ;\ (23,23) ;\ (10;13) ;\ (4;18)\\ &\Rightarrow (11,8) ;\ (1,4) ;\ (17,19) ;\ (4,18)\\ &\Rightarrow \text{LI} ;\ \text{BE} ;\ \text{RT} ;\ \text{ES}\\ &\Rightarrow \text{LIBERTES}\end{aligned}$$

Le mot cherché est donc : LIBERTÉ