Exercice 1 - Pondichéry 18 avril 2012

Partie A Restitution organisée de connaissance

Soient a, b, c, d des entiers relatifs et n un entier naturel non nul.

Si $a \equiv b \pmod{n}$, cela veut dire que $\exists k \in \mathbb{Z}$ tel que $a = n \times k + b$. Si de plus $c \equiv d \pmod{n}$, cela veut dire que $\exists k' \in \mathbb{Z}$ tel que $c = n \times k' + d$.

On peut en déduire que $a \times c = (n \times k + b) \times (n \times k' + d) = n \times k \times n \times k' + n \times k \times d + b \times n \times k' + b \times d = n(k \times n \times k' + k \times d + b \times k') + b \times d$ ce qui veut bien dire que $ac \equiv bd \pmod{n}$.□

Partie B Inverse de 23 modulo 26

1. Remplaçons x par -9 et y par -8 : $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$. Ainsi le couple $(-9\ ;\ -8)$ est solution de l'équation (E).□

2. On cherche tous les couples $(x\ ;\ y)$ solution de (E). Sachant que $23 \times (-9) - 26 \times (-8) = 1$, (E) est donc équivalente à :

$$\begin{aligned} 23x - 26y &= 23 \times (-9) - 26 \times (-8) \\ 23x + 23 \times 9 &= 26 \times 8 + 26y \quad \text{(+26y + 23 × 9)} \\ 23(x+9) &= 26(y+8) \quad \text{(On factorise)} \end{aligned}$$

   D'après cette écriture, il vient que $23|(26(y+8))$. Or $23 \wedge 26 = 1$ (car 23 est premier et ne divise pas 26), donc d'après le théorème de Gauss, $23|(y+8)$. Donc $\exists k \in \mathbb{Z}$ tel que $y + 8 = 23k$, soit $y = 23k - 8$.

   En remplaçant y par cette expression dans l'équation du dessus, il vient alors $23(x+9) = 26(23k)$, soit $x + 9 = 26k$ soit $x = 26k - 9$.

   Ainsi $\boxed{\mathcal{S} = \{(26k - 9\ ;\ 23k - 8) \text{ pour } k \text{ variant dans } \mathbb{Z}\}}$.

3. Quel que soit x premier entier d'un couple solution de (E), $23x \equiv 1 \pmod{26}$ (puisque $23x = 26y + 1$). Il suffit de trouver une valeur de k pour laquelle $0 \leq 26k - 9 \leq 25$: $k = 1$ convient, ce qui donne $\boxed{a = 17}$.

Partie C Chiffrement de Hill

1. $\underbrace{\text{ST}}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (18, 19) \overset{\text{étape 2}}{\Longrightarrow} (21, 20) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\boxed{\text{VU}}}_{\text{mot codé}}$

   Effectivement $11 \times 18 + 3 \times 19 = 255 = 9 \times 26 + 21$ et $7 \times 18 + 4 \times 19 = 202 = 7 \times 26 + 20$.

2. (a) Soit un couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_1).

   Alors $4y_1 + 23y_2 \equiv 4(11x_1 + 3x_2) + 23(7x_1 + 4x_2) = 44x_1 + 12x_2 + 161x_1 + 92x_2 = 205x_1 + 104x_2$

   Or $205 = 7 \times 26 + 23 \equiv 23 \pmod{26}$ et $104 = 4 \times 26 \equiv 0 \pmod{26}$.

   Ainsi $205x_1 \equiv 23x_1$ et $104x_2 \equiv 0$ d'où la ligne 1 de (S_2).

   Le même raisonnement donne également la ligne 2 de (S_2).□

   (b) Dans la partie B, on a vu que $23 \times 17 \equiv 1$. Multiplions donc le système de la question 2)a) par 17 :

   $23 \times 17 \equiv 1$ donc $23 \times 17x_1 \equiv x_1$ et $23 \times 17y_2 \equiv y_2$.

   $4 \times 17 = 68 = 2 \times 26 + 16 \equiv 16$, donc $4 \times 17y_1 \equiv 16y_1$, d'où la ligne 1 de (S_3).

   De même $19 \times 17 = 323 = 12 \times 26 + 11 \equiv 11$, donc $19 \times 17y_1 \equiv 11y_1$ d'où la ligne 2 de (S_3).

   (c) C'est exactement le même raisonnement qu'à la question 2)a) : à partir de (S_3) on multiplie x_1 par 11, x_2 par 3 pour obtenir la ligne 1 de (S_1), et on fait de même pour la ligne 2 de (S_1).

(d) Ainsi pour décoder le mot **YJ**, il suffit de chiffrer **YJ** à l'aide des étapes 1, 2 et 3 en remplaçant simplement (S_1) par (S_3) !

$$\underbrace{\text{YJ}}_{\text{mot en clair}} \overset{\text{étape 1}}{\Longrightarrow} (24,9) \overset{\text{étape 2}}{\Longrightarrow} (3,23) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\boxed{\text{DX}}}_{\text{mot codé}}$$

Effectivement $16\times 24+9 = 393 = 15\times 26+3$ et $11\times 24+5\times 9 = 309 = 11\times 26+23$.

Exercice 2

1. Pour avoir la liste des diviseurs positifs, on peut diviser 629 par les nombres entiers à partir de 1 et dès lors que la division a un reste nul, c'est que le nombre choisi était diviseur de 629 (et le quotient est un autre diviseur). Il est suffisant de s'arrêter à $\sqrt{629} \approx 25$ puisque, comme on l'a vu en cours, si $d > \sqrt{629}$ est un diviseur de 629, alors $\dfrac{629}{d} < \sqrt{629}$ en est un autre, et la méthode nous a déjà fait trouver d. On peut donc rentrer $Y_1 = 629/X$ et faire un tableau de valeurs pour X allant de 1 à 25 par pas de 1.

   Enfin pour avoir tous les diviseurs, on rajoute bien sûr les opposés :

   $\boxed{\mathcal{D}(629) = \{1; 629; 17; 37; -1; -629; -17; -37\}}$.

2. 32 200 est divisible par 2 : $32\ 200 = 2\times 16\ 100$.

   16 100 également : $16\ 100 = 2\times 8\ 050$

   8 050 également : $8\ 050 = 2\times 4025$.

   4 025 n'est pas divisible par 3, mais est divisible par 5 : $4\ 025 = 5\times 805$

   805 est divisible par 5 : $805 = 5\times 161$.

   161 est divisible par 7 : $161 = 7\times 23$, et 23 est premier.

   Ainsi $32\ 200 = 2\times 2\times 2\times 5\times 5\times 7\times 23 = \boxed{2^3\times 5^2\times 7\times 23}$

3. J'espère que vous avez reconnu l'exercice 110 p.71, que l'on avait traité en classe.

   (a) Si on appelle x le nombre de jetons de Zoé, l'énoncé se réécrit en $\boxed{x \equiv 9[17] \text{ et } x \equiv 3[5]}$.

   (b) $300 = 17\times 17 + 11$, donc $300 \equiv 11[17]$. Ainsi pour obtenir un nombre congru à 9 modulo 17, on peut rajouter 15 (car $15 \equiv -2[17]$ donc un nombre congru à 11 plus un nombre congru à -2 donne bien un nombre congru à 9 modulo 17).

   Effectivement $315 = 18\times 17+9$. Pour trouver les autres nombres de jetons x possibles pour que $x \equiv 9[17]$, il suffit ensuite de rajouter autant de fois 17 que l'on veut (et puisqu'on veut rester entre 300 et 400, on s'arrêtera à 400).

   Ainsi les possibilités pour être congru à 9 modulo 17 sont $\boxed{315\ ;\ 332\ ;\ 349\ ;\ 366\ ;\ 383\ ;\ 400}$.

   Il faut aussi trouver parmi ces nombres, ceux qui sont congrus à 3 modulo 5 !

   $315 = 63\times 5 + 0$ donc $315 \equiv 0[5]$

   $332 = 66\times 5 + 2$ donc $332 \equiv 2[5]$

   $349 = 69\times 5 + 4$ donc $349 \equiv 4[5]$

   $366 = 73\times 5 + 1$ donc $366 \equiv 1[5]$

   $383 = 76\times 5 + 3$ donc $383 \equiv 3[5]$

   $400 = 80\times 5 + 0$ donc $400 \equiv 0[5]$.

   Au final, la seule possibilité est que Zoé possède $\boxed{383 \text{ jetons}}$.