Contrôle de mathématiques

Mardi 18 décembre 2012

EXERCICE 1

ROC **3 points**

1) Démontrer le théorème de Gauss en utilisant le théorème de Bézout.
2) a et b sont deux entiers naturels non nuls tels que $a > b$.
   Démontrer que : $\text{pgcd}(a;b) = \text{pgcd}(a-b,b)$

EXERCICE 2

Application du cours **5 points**

1) Déterminer à l'aide de l'algorithme d'Euclide le pgcd de 1386 et 546. En déduire le ppcm de 1386 et 546
2) Montrer que les nombres 2013 et 734 sont premiers entre eux.
3) Démontrer que pour tout entier relatif n, les entiers $(14n+3)$ et $(5n+1)$ sont premiers entre eux. En déduire le pgcd(87,31).
4) Soit a et b deux entiers naturels tels que $a < b$. Déterminer a et b tels que : $\text{pgcd}(a,b) = 6$ et $\text{ppcm}(a,b) = 102$.

EXERCICE 3

BAC **4 points**

On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que

$$\begin{cases} N \equiv 5 \quad (13) \\ N \equiv 1 \quad (17) \end{cases}$$

1) Vérifier que 239 est solution de ce système.
2) Soit N un entier relatif solution de ce système.
   Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.
3) Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.
4) En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.

EXERCICE 4

Le chiffrement de Hill **8 points**

Partie A Inverse de 23 modulo 26

On considère l'équation : (E) : $23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1) Vérifier que le couple $(-9\ ;\ -8)$ est solution de l'équation (E).
2) Résoudre alors l'équation (E).
3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1 \pmod{26}$.

Partie B Chiffrement de Hill

Le chiffrement de Hill a été publié en 1929. C'est un chiffre polygraphique, c'est à dire qu'on ne chiffre pas les lettres les unes après le autres, mais par "paquets". On présente ici un exemple "bigraphique", c'est à dire que les lettres sont regroupées deux à deux.

Étape 1 On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient des couples d'entiers $(x_1\ ;\ x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

Étape 2 Chaque couple $(x_1\ ;\ x_2)$ est transformé en $(y_1\ ;\ y_2)$ tel que :

$$(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \quad \text{avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 Chapque couple $(y_1\ ;\ y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (19,4) \overset{\text{étape 2}}{\Longrightarrow} (13,19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1) Coder le mot ST.
2) On décide de construire un algorithme permettant d'aller plus vite. On propose l'algorithme suivant :
   a) Coder PALACE et RAPACE
   b) Que constatez-vous ?

Variables
X, Y, Z, T
Initialisation
Lire X, Y
traitement
$11 * X + 3 * Y \to Z$
$7 * X + 4 * Y \to T$
$Z - E\,(Z/26) * 26 \to Z$
$T - E\,(T/26) * 26 \to T$
Sortie
Afficher Z, T

3) On veut maintenant déterminer la procédure de décodage :
   a) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_1), vérifie les équations du système :

$$(S_2)\ \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases}$$

   b) À l'aide de la partie A, montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système

$$(S_3)\ \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$$

   c) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_3), vérifie les équations du système (S_1)
   d) Ecrire un algorithme sur le même principe que l'algorithme de chiffrage pour décoder un mot.
   e) Décoder le mot : PFXXKNU
   Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, on supprimera la lettre dont le code est W.