Correction contrôle de mathématiques

du jeudi 24 janvier 2019

EXERCICE 1

Questions de cours **(5 points)**

1) a) Deux entiers a et b sont premiers entre eux si, et seulement si, il existe une combinaison linéaire de a et b égal à 1 :

$$\text{pgcd}(a,b) = 1 \quad \Leftrightarrow \quad \exists (u,v) \in \mathbb{Z}^2, \quad au + bv = 1$$

b) $\forall n \in \mathbb{N}, \quad (-2)(7n+3) + 7(2x+1) = -14n - 6 + 14n + 7 = 1.$

Il existe une combinaison linéaire de $(7n+3)$ et $(2n+1)$ égal à 1 donc d'après le théorème de Bézout, les entiers $(7n+3)$ et $(2n+1)$ sont premiers entre eux.

2) Si un entier a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration : a divise bc, il existe $k \in \mathbb{Z}$ tel que : $bc = ka$.

a et b premiers entre eux, d'après le théorème de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que :

$$au + bv = 1 \overset{\times c}{\Rightarrow} auc + bvc = c \overset{bc=ka}{\Rightarrow} auc + kac = c \Rightarrow a(uc + kc) = c$$

On en déduit que a divise c.

3) a) Si deux entiers b et c divise a et si b et c sont premiers entre eux, alors bc divise a.

b) 5 et 11 divise $(n-9)$, d'après le corollaire du théorème de Gauss, $5 \times 11 = 55$ divise $(n-9)$. On a alors :

$$n - 9 \equiv 0 \ (55) \quad \Leftrightarrow \quad n \equiv 9 \ (55)$$

EXERCICE 2

Points de coordonnées entières sur une droite **(8 points)**

1) a) $y = \dfrac{5}{4}x - \dfrac{2}{3} \overset{\times 12}{\Leftrightarrow} 12y = 15x - 8 \Leftrightarrow 15x - 12y = 8.$

b) D'après le corollaire du théorème de Bézout, $15x - 12y = 8$ admet des solutions entières si, et seulement si $\text{pgcd}(15,12) = 3$ divise 8.
Ce n'est pas le cas, donc Δ_1 n'admet pas de point de coordonnées entières.

2) a) Si le point de coordonnées entières (x_0, y_0) est un point de Δ, alors :

$$y_0 = \frac{m}{n}x_0 - \frac{p}{q} \overset{\times nq}{\Leftrightarrow} nq\,y_0 = mq\,x_0 - pn \Leftrightarrow pn = mq\,x_0 - nq\,y_0 \Leftrightarrow pn = q\,(mx_0 - ny_0)$$

Donc q divise pn.

b) On sait que p et q sont premiers entre eux, donc d'après le théorème de Gauss, q divise n.

3) Réciproquement :

a) On sait que n et m sont premiers entre eux, donc d'après le théorème de Bézout, il existe $(u,v') \in \mathbb{Z}^2$ tel que : $nu + mv' = 1 \Rightarrow qru - m(-v') = 1 \overset{v=-v'}{\Rightarrow} qru - mv = 1.$

b) On a vu à la question 2a) que l'équation de Δ est équivalente à :

$$pn = q(mx_0 - ny_0) \overset{n=qr}{\Leftrightarrow} pqr = q(mx_0 - ny_0) \overset{\div q \neq 0}{\Leftrightarrow} pr = mx_0 - ny_0$$

On a vu à la question 3a) que :

$$nu - mv = 1 \overset{\times pr}{\Leftrightarrow} nupr - mvpr = pr \Leftrightarrow pr = m(-vpr) - n(-upr)$$

En identifiant les deux forme le point de coordonnée $(-vpr\ ;\ -upr)$ est solution de Δ

4) a) Δ admet un point de coordonnées entières si et seulement si q divise n.

b) $y = \frac{3}{8}x - \frac{7}{4}$ donc $q = 4$ et $n = 8$.

Comme 4 divise 8, (Δ_2) possède un point de coordonnées entières.

EXERCICE 3

Chiffrement affine **(7 points)**

1) $L \rightarrow 11 \overset{f}{\rightarrow} 82 = 26 \times 3 + 4 \overset{\equiv (26)}{\rightarrow} 4 \rightarrow E.$

L se code avec la lettre E.

2) a) Par double implication :

$$7x \equiv m\ (26) \overset{\times 15}{\Rightarrow} 105x \equiv 15m\ (26) \overset{105=26\times 4+1}{\Rightarrow} x \equiv 15m\ (26)$$

Réciproquement :

$$x \equiv 15m\ (26) \overset{\times 7}{\Rightarrow} 7x \equiv 105m\ (26) \overset{105=26\times 4+1}{\Rightarrow} 7x \equiv m\ (26)$$

b) $y \equiv 7x + 5\ (26) \Leftrightarrow 7x \equiv y - 5 \overset{2a)}{\Leftrightarrow} x \equiv 15y - 75\ (26) \overset{-75=26(-3)+3}{\Leftrightarrow} x \equiv 15y + 3\ (26).$

La fonction de décodage f^{-1} est définie par : $f^{-1}(y) = 15y + 3$.

3) $F \rightarrow 5 \overset{f^{-1}}{\rightarrow} 78 = 26 \times 3 + 0 \overset{\equiv (26)}{\rightarrow} 0 \rightarrow A.$

F se décode avec la lettre A.

4) On a :

I	Y	Y	Q
2	2	5	6

Cela revient à appliquer 6 fois la fonction de décodage à la lettre Q(16).

On peut remplir le tableau suivant :

y	$f^{-1}(y)$	x
16	243	9
9	138	8
8	123	19
19	288	2
2	33	7
7	108	4

Avec ce système de codage Q se décode en E(4).

Remarque : IYYQ se décode en "CODE".