# CORRECTION DU DS

## Exercice 1.

**1)** Déterminer le plus petit entier positif dont le reste lors de la division euclidienne par 5 et par 11 est égal 2.

On veut que $n-2$ soit divisible par 5 et 11. Comme $PGCD(5,11)=1$ on en déduit que $n-2$ est divisible par 55 ; d'où $n-2=55z$ avec $z\in\mathbb{Z}$. On en déduit que $n=2+55z$ et par conséquent que le plus petit entier positif vérifiant les hypothèses est 2.

**2)** Qu'impliquent les résultats suivants :

$5\,|\,ab$ ?

D'après une conséquence du lemme de Gauss comme 5 est premier on en déduit que 5 divise $a$ ou 5 divise $b$.

$15\,|\,ab$ ?

On en déduit que 5 divise $ab$ et 3 divise $ab$, et par conséquent 5 divise $a$ ou $b$ et 3 divise $a$ ou $b$.

**3)** Soit $a$ et $b$ deux entiers. Que peut-on en déduire pour le PGCD de $a$ et $b$ si $12a+25b=15$ ?

On en déduit que $PGCD(a,b)$ divise 15.
Par exemple si $a=-5$ et $b=3$ on a
$12a+25b=15$ et $PGCD(a,b)=PGCD(-5,3)=PGCD(5,3)=1$.

**4)** Soit $a$ et $b$ deux entiers. Que peut-on en déduire pour $a$ et $b$ si on a $\mathrm{PGCD}(a,b)=8$ et $\mathrm{PPCM}(a,b)=40$ ?

On a $|ab|=PGCD(a,b)PPCM(a,b)=320$

**5)** Soit $a$ et $b$ deux entiers. Expliquer pourquoi on a $\mathrm{PGCD}(a,b)\,|\,\mathrm{PPCM}(a,b)$.

On a $PGCD(a,b)$ divise $a$ et $a$ divise $PPCM(a,b)$, d'où le résultat.

## Exercice 2.

**1.** Soit $n$ un entier strictement positif. Déterminer le reste $R_1$ de la division euclidienne de $21n+4$ par $14n+3$ ; puis le reste $R_2$ de la division de $14n+3$ par $R_1$.

Lorsqu'on effectue les divisions euclidiennes on obtient :
$21n+4=(14n+3).1+7n+1$ et $14n+3=(7n+1).2+1$ d'où $R_1=7n+1$ et $R_2=1$.

**2.** Pour $n\in\mathbb{N}^*$ déterminer $PGCD(14n+3,21n+4)$. Que peut-on en déduire pour les entiers $14n+3$ et $21n+4$.

D'après ce qui précède $PGCD(21n+4,14n+3)=1$ et donc $14n+3$ et $21n+4$ sont premiers entre eux.

**3.** Donner une solution $(u,v)$ de l'identité de Bézout $(14n+3)u+(21n+4)v=1$.

On a
$1=14n+3-(7n+1).2=14n+3-(21n+4-(14n+3)).2$
et donc
$1=(14n+3).3+(21n+4)(-2)$.
Une solution de l'identité de Bézout est donc $(u,v)=(3,-2)$.

**Exercice 3.**

**1.** Définir le chiffrement par décalage.

On considère les ensembles des messages en clair, des cryptogrammes et des clefs égaux à $\mathbb{Z}/26\mathbb{Z}$. Pour un message en clair $M = x_0x_1 \dots x_n$ et pour une clef $k$ le cryptogramme $C = y_0y_1 \dots y_n$ s'obtient par : $y_i = x_i + k \bmod 26$ pour $0 \leq i \leq n$.

**2.** Déterminer la message en clair, le cryptogramme, ainsi que la clef du chiffrement correspondant aux données ci-dessous, sachant que l'on a utilisé un chiffrement par décalage.

On remarque que $S$ (18) est remplacé par $D$ (3) donc la clef est $k = 3 - 18 = 11 \bmod 26$.
On en déduit alors que $C$, $R$ et $E$ sont codés par $N$, $C$ et $P$ car
$2 + 11 = 13 \bmod 26$, $18 + 11 = 3 \bmod 26$ et $4 + 11 = 15 \bmod 26$.
Pour déchiffrer il faut retrancher 11 aux valeurs des lettres du cryptogramme, ainsi on obtient par exemple pour $S$ : $18 - 11 = 7 \bmod 26$ qui correspond à $H$. Ceci nous donne le résultat suivant :

| message en clair | C | H | I | F | F | R | E | D | E | C | E | S | A | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| message chiffré | N | S | T | Q | Q | C | P | O | P | N | P | D | L | C |

**Exercice 4.**

On définit un système de chiffrement de la manière suivante ; si on a un message de longueur $k$, $M = m_om_1m_2 \dots m_k$ il est remplacé par le cryptogramme $C = c_0c_1c_2 \dots c_k$ défini par

$$\forall i,\ 0 \leq i \leq k, \quad c_i = m_i + i \bmod 26.$$

**1.** Quel est ce système de chiffrement ?

C'est un chiffrement de Vigenère

**2.** Déchiffrer le message **CFUWPJIOQOPCQZSCJUWOCBAKCQE** sachant qu'il a été obtenu à l'aide de ce chiffrement ?

On a $m_i = c_i - i \bmod 26$, d'où l'on obtient comme message en clair :

c'est le chiffrement de Vigenère.

********** **FIN** **********