

PROJET DS

ATTENTION LES CALCULS DOIVENT APPARAÎTRE SUR LES COPIES

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.

2) Qu'impliquent les résultats suivants :

$$5 \mid ab ?$$

$$15 \mid ab ?$$

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

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

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

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 .

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

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

Exercice 3.

On rappelle qu'on a la numérotation des lettres de l'alphabet suivante :

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

1. Définir le chiffrement par décalage.

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.

message en clair	C					R			E			S		R
message chiffré		S	T	Q	Q		P	O		N	P	D	L	

Exercice 4.

On définit un système de chiffrement de la manière suivante ; si on a un message de longueur k , $M = m_0 m_1 m_2 \dots m_k$ il est remplacé par le cryptogramme $C = c_0 c_1 c_2 \dots c_k$ défini par

$$\forall i, 0 \leq i \leq k, \quad c_i = m_i + i \pmod{26}.$$

1. Quel est ce système de chiffrement ?



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

