

Olympiades mathématiques de première 2017.

Sujet académique de Amiens.

I Exercice académique : langage codé.

Pour coder un message afin de le garder secret, on utilise la méthode de chiffrement suivante.

- On remplace chaque lettre du message par son rang indiqué dans le tableau ci-dessous.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Les autres signes (virgules, espaces, points,...) sont supprimés.

- On calcule le reste y de la division euclidienne de $7x + 5$ par 26.
- On remplace la lettre initiale x par celle ayant pour rang y .

Cette technique de codage est appelée *chiffrement affine*.

1. Vérifier, qu'en effectuant la division euclidienne de 89 par 26, on obtient 3 comme quotient et que le reste est 11.

En déduire que, par cette méthode, la lettre M est codée par la lettre L.

2. Coder le mot MATHS.
3. On admet la propriété suivante que l'on pourra utiliser lorsque nécessaire dans toute la suite de l'exercice :

Soient a et b deux entiers relatifs et c un entier naturel non nul.
 a et b ont le même reste dans la division euclidienne par c si et seulement si $a - b$ est un multiple de c .

Montrer que, pour tout entier relatif k , si a et b ont le même reste dans la division euclidienne par c alors les entiers ka et kb ont le même reste dans la division euclidienne par c .

4. Soient x et y des entiers.
 - (a) Montrer que si y et $7x$ ont le même reste dans la division euclidienne par 26 alors $15y$ et x ont le même reste dans la division euclidienne par 26.

(b) Démontrer la réciproque de l'implication précédente.

5. Dédurre alors que : y et $7x + 5$ ont même reste dans la division euclidienne par 26 équivaut à x et $15y + 3$ ont même reste dans la division euclidienne par 26.
6. À l'aide de la question précédente, décoder le mot ZERLGJFAHB.

Déchiffrer un message codé par un chiffrement affine ne pose pas de difficulté. La cryptographie utilise des techniques bien plus complexes pour crypter des textes ou des données et en assurer l'inviolabilité.