MESSAGES CODÉS

Commentaire : Utiliser la congruence pour coder/décoder un message à l’aide d’un chiffrement affine.



****Pour effectuer un codage affine d’une phrase, on associe à chaque lettre de l’alphabet un nombre entier compris entre 0 et 25.

Et, on note **\*** le séparateur entre deux mots ; on lui associe l’entier 26.

On a ainsi le tableau de correspondance ci-contre.

**PARTIE 1**

On associe à chaque valeur de $x$ le reste $y $de la division euclidienne de 4$x+3$ par $27$. Le caractère initial de rang $x$ de la phrase non codée est alors remplacé par le caractère de rang $y$ de la phrase codée.

On appelle ce codage « chiffrement affine de type $ax+b$ modulo $27$, avec $a=4$ et $b=3$ ».

**POUR CODER**

Écrire une relation de congruence exprimant $y$ en fonction de $x$.

➜ Coder alors la phrase « MATHS\*EXPERTES ».

**POUR DÉCODER**En déduire une relation de congruence exprimant $x$ en fonction de $y$.
➜ Décoder alors la phrase « FB\*TVZ\*DC\*ZFJ ».

**PARTIE 2**



On a codé la phrase suivante à l’aide d’un chiffrement affine modulo $27$

avec $a=7$ et $b=1$. Décoder cette phrase.

ZYGTVHVBVWCVQMGHCMCVZYGTVHVBVWCV\*MSGT

C\*VZYGTVHVBVWCV\*MSGTVESDLTVHVBVWCVQMGHCMC

WSLPVZYGTVHVBVWCVQMGHCMCVESDLTVHVBVWCVQMGHCMC

Hors du cadre de la classe, aucune reproduction, même partielle, autres que celles prévues à l'article L 122-5 du code de la propriété intellectuelle, ne peut être faite de ce site sans l'autorisation expresse de l'auteur.

[*www.maths-et-tiques.fr/index.php/mentions-legales*](http://www.maths-et-tiques.fr/index.php/mentions-legales)