**Exercice 1 : Déchiffrer avec l’inverse modulaire de *a***

Pré requis : Règles d’opérations sur les congruences.

Objectifs : Utiliser les opérations sur les congruences. Utiliser l’inverse modulaire pour simplifier.

* On code les lettres de l’alphabet en entiers naturels avec la table de codage suivante :

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F |  | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

* On considère la fonction de chiffrement définie sur où est le reste de la division de par .

On remarque qu’on a alors la relation de congruence simplifiée : .

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F |  | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
|  | 22 | 13 | 4 | 21 | 12 | 3 |  | 23 | 14 | 5 |
|  |  |  |  |  |  |  |  |  |  |  |

* Par lecture inverse de la table de codage, on déduit de la lettre chiffrée :

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F |  | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
|  | 22 | 13 | 4 | 21 | 12 | 3 |  | 23 | 14 | 5 |
| Lettre chiffrée | W | N | E | V | M | D |  | X | O | F |

1. Chiffrer le mot GRIS
2. On considère un entier[[1]](#footnote-2) tel que .
   1. Démontrer que est impair.
   2. Déterminer .
3. En déduire l’expression d’une fonction de déchiffrement de dans telle que :

***Méthode :***

* On isole dans en multipliant les deux membres par .
* On utilise la propriété « Dans une relation de congruence, on peut remplacer un des nombres par un autre qui lui est congru »

1. Déchiffrer le mot SWZQ.

1. Un tel entier *u* est **l’inverse modulaire** de 17 pour la multiplication modulo 26 [↑](#footnote-ref-2)