**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 $26$ lettres de l’alphabet en $26$ entiers naturels $x$ avec la table de codage suivante :

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F | $$…$$ | X | Y | Z |
| $$x$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ | $$4$$ | $$5$$ | $$…$$ | $$23$$ | $$24$$ | $$25$$ |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

* On considère la fonction de chiffrement $f:x⟼y=f(x)$ définie sur $\left\{0;1;2;…;24;25\right\}$ où $y$ est le reste de la division de $17x+22$ par $26$.

On remarque qu’on a alors la relation de congruence simplifiée : $y≡17x+22 (26)$.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F | $$…$$ | X | Y | Z |
| $$x$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ | $$4$$ | $$5$$ | $$…$$ | $$23$$ | $$24$$ | $$25$$ |
| $$y$$ | 22 | 13 | 4 | 21 | 12 | 3 |  | 23 | 14 | 5 |
|  |  |  |  |  |  |  |  |  |  |  |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre en clair | A | B | C | D | E | F | $$…$$ | X | Y | Z |
| $$x$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ | $$4$$ | $$5$$ | $$…$$ | $$23$$ | $$24$$ | $$25$$ |
| $$y$$ | 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) $u$ tel que $17u≡1 (26)$.
	1. Démontrer que $u$ est impair.
	2. Déterminer $u$.
3. En déduire l’expression d’une fonction de déchiffrement $g:y⟼x=g(y)$ de $\left\{0;1;2;…;24;25\right\}$ dans $\left\{0;1;2;…;24;25\right\}$ telle que : $y=f\left(x\right) ⇔ x=g\left(y\right) $

***Méthode :***

* On isole $x$ dans $y≡17x+22 (26)$ en multipliant les deux membres par $u$.
* 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)