Thème : Quelques applications des congruences

Activité 3. Déchiffrement affine (2 exercices)

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 $f: x \longmapsto y = f(x)$ définie sur $\{0; 1; 2; \dots; 24; 25\}$ où y est le reste de la division de $17x + 22$ par 26.

On remarque qu'on a alors la relation de congruence simplifiée : $y \equiv 17x + 22 \quad (26)$.

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] u tel que $17u \equiv 1 \quad (26)$.
   a) Démontrer que u est impair.
   b) Déterminer u.
3) En déduire l'expression d'une fonction de déchiffrement $g: y \longmapsto x = g(y)$ de $\{0; 1; 2; \dots; 24; 25\}$ dans $\{0; 1; 2; \dots; 24; 25\}$ telle que : $\quad y = f(x) \quad \Leftrightarrow \quad x = g(y)$

> ***Méthode :***
> - On isole x dans $y \equiv 17x + 22 \quad (26)$ 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 »

4) Déchiffrer le mot SWZQ.

[1] Un tel entier *u* est **l'inverse modulaire** de 17 pour la multiplication modulo 26

Exercice 2 : Chiffrer avec un algorithme, déchiffrer avec un tableur

Pré requis : connaissance des fonctions CODE, MOD et CAR des tableurs vues dans l'activité 2 du thème « Avant les congruences ».

Objectifs : Réinvestir les connaissances sur les algorithmes et les tableurs.

Partie A
Soit l'algorithme :

Déclaration des variables

a, b, c sont des entiers naturels

Début d'algorithme

Affecter à c la valeur 0

Demander la valeur de a

Demander la valeur de b

Tant que $a \geq b$

Affecter à c la valeur $c + 1$

Affecter à a la valeur $a - b$

Fin Tant que

Afficher c et a

Fin d'algorithme

1) Déterminer les valeurs affichées par cet algorithme pour $a = 25$ et $b = 7$ en recopiant et en complétant le tableau suivant :

c	a	b
0		
	25	
		7

2) Que calcule cet algorithme à partir de a et b ?

Partie B

On choisit, pour coder les lettres de l'alphabet, la table de codage suivante :

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

On définit le procédé de chiffrement affine suivant :

Etape n°1 : On code la lettre du message en clair avec le nombre m correspondant dans la table de codage.

Etape n°2 : On calcule le reste de la division de $3m + 5$ par 26. On note p ce reste.

Etape n°3 : On décode le nombre p à l'aide de la table de codage. Cela fournit la lettre du message chiffré.

1) Chiffrer la lettre **L**.

2) Ecrire un algorithme (en exploitant l'algorithme de la partie A) qui effectue les tâches suivantes :
   - Demander la valeur de m
   - Afficher la valeur de p

Partie C

1) En remarquant que $3 \times 9 \equiv 1 \quad [26]$, Démontrer que les propositions suivantes sont *équivalentes* :

* $3m + 5 \equiv p \quad [26]$
* $m \equiv 9p + 7 \quad [26]$

2) Déchiffrer la lettre **M**.

Partie D

En utilisant les fonctions CODE, MOD et CAR d'un tableur, déchiffrer le message suivant :

M R H H F S X M V K H M V S X H O R H Q D V M V S H O R M F N K V P S R