# Thème : Quelques applications des congruences

## Corrigé de l’activité 7.

**Exercice 1 : *Chiffrement de Hill***

Voir le fichier tableur pf5372b07.chiffrement\_de\_hill\_tableur.xls ou pf5372b07.chiffrement\_de\_hill\_tableur.ods

**Partie A** *Chiffrement*

1. On fait le tableau des rangs des 26 lettres de l’alphabet :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre | A | B | C | D | E | F | G | H | I | J | K | L | M |
| Rang | 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 |

* La matrice contient les rangs du couple de lettres en clair .

Posons

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Le reste de la division de par est .

Le reste de la division de par est .

Donc . contient les rangs du couple de lettres chiffrées .

Ainsi, le mot "CD" est chiffré en "**VT**".

1. Chiffrement avec la même clé du mot « AX »

* La matrice contient les rangs du couple de lettres en clair .

Posons

On obtient à la calculatrice .

Le reste de la division de par est .

Le reste de la division de par est .

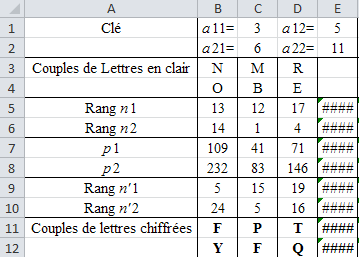
Donc . contient les rangs du couple de lettres chiffrées .

Ainsi, le mot "AX" est chiffré en "**LT**".

1. Avec les exemples précédents, on voit que pour deux mots en clair aux lettres toutes distinctes, obtient dans les deux mots chiffrés la lettre T plusieurs fois.

Donc deux lettres distinctes ne sont pas chiffrées en deux lettres distinctes.

1. On réalise le tableau suivant avec un tableur : Voir le fichier chiffrement\_de\_hill\_tableur

****

* La cellule B5 contient la formule =CODE(B3)-65

La cellule B6 contient la formule =CODE(B4)-65

Formules du produit matriciel .

Le $ permet de fixer la référence de la colonne ou de la ligne lors de la recopie automatique.

}

* La cellule B7 contient la formule =$C1\*B$5+$E1\*B$6

La cellule B8 contient la formule =$C2\*B$5+$E2\*B$6

* La cellule B9 contient la formule =MOD(B7;26)

La cellule B10 contient la formule = MOD(B8;26)

* La cellule B11 contient la formule =CAR(B9+65)

La cellule B12 contient la formule = CAR(B10+65)

Le mot « NOMBRE » est chiffré en « **FYPFTQ**».

**Partie B** *Déchiffrement*

1. Par lecture de la table de codage de la question 1) de la partie A, on a :
2. a) On a :
   1. On a :

avec . Donc . Donc la matrice est inversible.

* 1. La matrice inverse de est .
  2. A la calculatrice, on obtient :

|  |  |  |
| --- | --- | --- |
|  |  |  |

* 1. La clé donne des matrices à coefficients parfois non entiers. Elle ne permet donc pas le déchiffrement.

1. On effectue les produit matriciels :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | |  |
|  |  | | contient les rangs du couple de lettres en clair . | |
|  |  | | contient les rangs du couple de lettres en clair . | |
|  |  | | contient les rangs du couple de lettres en clair . | |

La clé permet donc le déchiffrement du message « **FYPFTQ**»

*Remarque :*

On peut se demander d’où vient la matrice .

donc est la comatrice transposée de , c’est à dire

Dans l’exemple, . Le coefficient est l’inverse de modulo ce qui permet de simplifier les relations de congruence.

De façon générale, toute matrice dont le déterminant est premier avec convient comme clé de chiffrement puisque dans ce cas a un inverse modulo .

1. • Considérons le chiffrement d’un couple de lettres en clair quelconques, de rangs . et sont des entiers appartenant à . Considérons la clé de chiffrement .

|  |  |
| --- | --- |
| On définit la matrice |  |

* + Pour chiffrer, on calcule la matrice

|  |  |
| --- | --- |
|  |  |

* + Pour trouver les rangs des lettres du couple chiffré, on calcule la matrice

|  |  |
| --- | --- |
|  | où et sont des entiers appartenant à . |

* Considérons le déchiffrement du couple de lettres chiffrées de rangs avec la clé de déchiffrement où

|  |  |
| --- | --- |
| On a |  |

* + Pour déchiffrer, on calcule la matrice
  + Montrons que cette matrice permet de toujours obtenir les rangs et du couple de lettres en clair.

Or, de par la méthode de chiffrement, on a

Donc, les facteurs qui apparaissent dans la matrice vérifient

On retrouve les éléments de la matrice en multipliant les deux membres par (qui est l’inverse de modulo ) :

Et comme

Ainsi :

|  |  |
| --- | --- |
|  | où et sont des entiers appartenant à . |

*Conclusion :*

La clé avec et permet de déchiffrer tous les messages chiffrés avec la clé

1. Déchiffrement du message « **MPYORQZL** »

* La matrice contient les rangs du couple de lettres

On déchiffre ce couple en faisant le produit .

On obtient à la calculatrice .

donc

contient les rangs du couple de lettres en clair .

* La matrice contient les rangs du couple de lettres

On déchiffre ce couple en faisant le produit .

On obtient à la calculatrice .

donc

contient les rangs du couple de lettres en clair .

* La matrice contient les rangs du couple de lettres

On déchiffre ce couple en faisant le produit .

On obtient à la calculatrice .

donc

contient les rangs du couple de lettres en clair .

* La matrice contient les rangs du couple de lettres

On déchiffre ce couple en faisant le produit .

On obtient à la calculatrice .

donc

contient les rangs du couple de lettres en clair .

Ainsi le message déchiffré est « TRESBIEN ».

**Exercice 2 : *Chiffrement RSA***

**Partie A :** Alice décide de choisir (*n* ; *e*) = (21 ; 5) comme clé publique.

1. a) Elle peut effectivement faire ce choix, en effet :

* 21 est égal au produit de deux nombres premiers : . On a .
* On a alors et est premier avec 12 et 5 est compris entre 1 et 12.
  1. Le choix de ne permet pas d'assurer la sécurité du message. Il est en effet beaucoup trop simple de factoriser et donc de déterminer une clé privée.

1. a) On a .
   1. tel que .

Or

5 et 12 sont premiers entre eux donc d'après le théorème de Bézout, l'équation (*E*) admet des solutions.

* 1. Soit par essais successifs, soit en utilisant la calculatrice, soit en utilisant l'algorithme d'Euclide, on peut trouver : comme solution particulière de l'équation .
  2. Résolution de l'équation : .

Or 5 et 12 sont premiers entre eux et 5 divise donc d'après le théorème de Gauss, 5 divise  
 donc il existe un entier tel que et donc il existe un entier tel que .

De plus, ; on a alors .

On a donc

Les solutions de l'équation (*E*) sont donc les entiers appartenant à .

* 1. Parmi les clés privées proposées, la seule possible est donc (21 ; 17). Alice a choisi . Elle utilisera par la suite cette clé pour déchiffrer les messages de Bob.

1. a) En associant à chaque lettre du mot PAL, sa place dans l'alphabet, on trouve :
   1. Par définition, et . Donc .

De même, on a .

* 1. Le message chiffré envoyé par Bob : 4 1 3.

1. a) La clé privée de déchiffrement est (21 ; 17).

On sait que avec . Donc . On a de même .

* 1. En associant les lettres correspondantes, le message envoyé par Bob était donc PAL.

**Partie B :** Alice a choisi (55 ; 3) comme clé privée.

1. Dans Liste3, ce sont les restes de la division par 55 des entiers de Liste1 élevés à la puissance 3 qui sont calculés.
2. La séquence de touches pour obtenir les trois listes est la suivante :

|  |  |
| --- | --- |
| Sur calculatrice TI (TI 82 – 83)   * Appuyer sur la touche Stats   Dans le menu EDIT, choisir 4: EffListe  Effacer les listes L1, L2, L3 précédentes en saisissant EffListe L1,L2,L3 entrée   * Appuyer sur la touche Stats   Dans le menu EDIT, choisir 1: EDIT   * Amener le curseur sur le titre de la colonne L1 entrée   2nd Listes , OP, 5: suite entrée  Saisir suite(X,X,1,54,1) entrée  La colonne L1 se remplit des entiers de 1 à 54.   * Amener le curseur sur le titre de la colonne L2 entrée   Dans la zone en bas, à gauche de L2=, taper la formule L1^3 entrée  La colonne L2 se remplit des cubes des éléments de L1   * Amener le curseur sur le titre de la colonne L3 entrée   Dans la zone en bas, à gauche de L3=, taper la formule L2  55\*partEnt(L2/55) entrée  La colonne L3 se remplit des restes de la division des éléments de L2 par 55. | Sur calculatrice Casio (GRAPH 35+ USB)   * Aller dans le menu **STAT**   Effacer les List 1 List 2 List 3 précédentes en mettant en surbrillance un élément de ces listes. Appuyer sur F6, aller dans DEL-A (touche F4) et valider "Yes".  Amener le curseur sur le Titre de la première Liste List 1   * Aller dans le menu **RUN-MAT** * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis Seq (touche F5)  Saisir Seq(X,X,1,54,1) → List 1 puis appuyer sur EXE  SHIFT QUIT   * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis ( puis List (touche F1)  Saisir (List 1)^3 → List 2 puis appuyer sur EXE  SHIFT QUIT   * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis ( puis List (touche F1)  Saisir (List 2)  55×Intg((List 2)÷55) → List 3 puis appuyer sur EXE  SHIFT QUIT   * Aller dans le menu **STAT**   Vérifier que les List 1 List 2 List 3 sont correctement remplies. |

On obtient :

|  |  |  |
| --- | --- | --- |
| Liste 1 (Codes chiffrés | Liste 2 (calcul intermédiaire) | Liste3 (Codes en clair |
| **1** | 1 | **1** |
| 2 | 8 | 8 |
| 3 | 27 | 27 |
| 4 | 64 | 9 |
| **5** | 125 | **15** |
| 6 | 216 | 51 |
| … | … | … |

1. Le tableau précédent permet donc à Alice de déchiffrer le message reçu.

A chaque valeur codant le message chiffré (*C*) qui a été envoyé par Bob, le tableau permet d'associer la valeur codant la lettre en clair à lire dans la troisième colonne.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (*C*) code chiffré | 10 | **1** | 7 | 25 | 24 | 18 | **5** | 9 | 49 |
| (*M*) code en clair | 10 | **1** | 13 | 5 | 19 | 2 | **15** | 14 | 4 |
| Lettre en clair | **J** | **A** | **M** | **E** | **S** | **B** | **O** | **N** | **D** |

**Partie C :** Alice a choisi (221 ; 35) comme clé privée.

1. Dans Liste3, ce sont les restes de la division par 221 des entiers de Liste1 élevés à la puissance 35.

La séquence de touches pour obtenir les trois listes est la suivante :

|  |  |
| --- | --- |
| Sur calculatrice TI (TI 82 – 83)   * Appuyer sur la touche Stats   Dans le menu EDIT, choisir 4: EffListe  Effacer les listes L1, L2, L3 précédentes en saisissant EffListe L1,L2,L3 entrée   * Appuyer sur la touche Stats   Dans le menu EDIT, choisir 1: EDIT   * Amener le curseur sur le titre de la colonne L1 entrée   2nd Listes , OP, 5: suite entrée  Saisir suite(X,X,1,220,1) entrée  La colonne L1 se remplit des entiers de 1 à 220.   * Amener le curseur sur le titre de la colonne L2 entrée   Dans la zone en bas, à droite de L2=, taper la formule L1^35 entrée  La colonne L2 se remplit des puissances 35 des éléments de L1   * Amener le curseur sur le titre de la colonne L3 entrée   Dans la zone en bas, à droite de L3=, taper la formule L2 221\*partEnt(L2/221) entrée  La colonne L3 se remplit des restes de la division des éléments de L2 par 221. | Sur calculatrice Casio (GRAPH 35+ USB)   * Aller dans le menu **STAT**   Effacer les List 1 List 2 List 3 précédentes en mettant en surbrillance un élément de ces listes. Appuyer sur F6, aller dans DEL-A (touche F4) et valider "Yes".  Amener le curseur sur le Titre de la première Liste List 1   * Aller dans le menu **RUN-MAT** * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis Seq (touche F5)  Saisir Seq(X,X,1,220,1) → List 1 puis appuyer sur EXE  SHIFT QUIT   * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis ( puis List (touche F1)  Saisir (List 1)^35 → List 2 puis appuyer sur EXE  SHIFT QUIT   * Appuyer sur la touche OPTN   Aller dans LIST (touche F1) puis ( puis List (touche F1)  Saisir (List 2)  221×Intg((List 2)÷221) → List 3 puis appuyer sur EXE  SHIFT QUIT   * Aller dans le menu **STAT**   Vérifier que les List 1 List 2 List 3 sont correctement remplies. |

|  |  |  |  |
| --- | --- | --- | --- |
| On obtient : | Liste 1 (Codes chiffrés | Liste 2 (calcul intermédiaire) | Liste3 (Codes en clair |
|  | 1 | 1 | 1 |
|  | 2 | 3.4E10 | 59 |
|  | **3** | **5E16** | **0** |
|  | 4 | 1.2E21 | 0 |
|  | 5 | 2.9 E 24 | 0 |
|  | 6 | 1.7 E 27 | 0 |
|  | … | … | … |

Les valeurs dans la troisième liste peuvent être nulles à cause d'un dépassement de la taille des nombres que la calculatrice est capable de stocker. Dans ce cas, l'affichage de la liste 3 ne permet pas de déchiffrer.

|  |  |  |
| --- | --- | --- |
| Soit . | (calcul intermédiaire) | Le reste dans la division de par (Code en clair |
| Affichage calculatrice |  | 0 - valeur fausse - |
| Valeur exacte | 50031545098999707 | 61 - valeur correcte - |

Pour calculer le reste d'une division euclidienne, il est impératif de ne travailler qu'avec des valeurs exactes !   
Or la calculatrice ne permet pas de le faire au-delà de nombres entiers de plus de 13 chiffres.

1. a) On sait que pour tout entier naturel , et donc si alors d'après la compatibilité des congruences et de la multiplication, on a

Donc, si alors.

* 1. L'algorithme complété :

ENTREE :

entier naturel

TRAITEMENT ET SORTIE :

Saisir

*R* prend la valeur **1**

Pour *I* allant de 1 à **35**

prend la valeur partEnt

Fin Pour

Afficher

1. Le programme sur la calculatrice :

Programme PUISSANC sur TI

Prompt C

1R

For(I,1,35)

R\*C221\*PartEnt(R\*C/221)R

End

Disp R

Programme PUISSANC sur Casio

"C="?→C

1→R

For 1I To 35

R×C221×Intg(R×C/221)R

Next

R◢

ClrText

En utilisant ce programme Alice associe à chaque valeur du message (*C*) envoyé la valeur affichée. Elle obtient :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 126 | 164 | 208 | 164 | 76 | 76 | 1 | 184 | 164 | 27 | 164 | 76 | 1 |
|  | 3 | 5 | 13 | 5 | 19 | 19 | 1 | 7 | 5 | 14 | 5 | 19 | 1 |
| (*M*) en clair | C | E | M | E | S | S | A | G | E | N | E | S | A |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 200 | 41 | 111 | 166 | 164 | 41 | 86 | 200 | 185 | 86 | 1 | 152 | 1 | 76 |
| 21 | 20 | 15 | 4 | 5 | 20 | 18 | 21 | 9 | 18 | 1 | 16 | 1 | 19 |
| U | T | O | D | E | T | R | U | I | R | A | P | A | S |