Le chiffrement affine

Objectifs:

- Introduire la notion de congruence
- Introduire les propriétés algébriques des congruences
- Prolonger avec un algorithme et une programmation

Enoncé « élèves »

On chiffre les lettres de l'alphabet en leur associant dans l'ordre un entier entre 0 et 25 :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Le principe du codage :

- l'expéditeur **écrit le message sous une forme numérique** x selon le principe ci-dessus.
- L'expéditeur **code** le message en utilisant une fonction affine , on note y
- Le récepteur **décode** y pour retrouver x à partir duquel il retrouve le message
-

Partie A : Le codage

On souhaite coder à l'aide d'un tableur le message « bonjour » en utilisant la fonction f définie par $f(x)=19x+3$

Définition : Le code ASCII (American Standart Code for Information Interchange) est un codage numérique des caractères. Les lettres minuscules sont codées de 97 à 122 et les majuscules de 65 à 90. Les tableurs et Xcas utilisent ce type de codage.

Avec Excel ou LibreOfficeCalc :

le fonction CODE associe à chaque lettre minuscule de l'alphabet un entier entre 97 et 122.
par exemple CODE (« a ») ENTREE donne 97.

1° Faire apparaître les lettres de « bonjour » en minuscule sur une ligne du tableur puis sur la ligne suivante le message numérisé en x, entier entre 0 et 25

2° Sur une nouvelle ligne faire apparaître le chiffrement y' tel que $y' = 19x + 3$. L'entier y' permet -il toujours d'associer immédiatement une lettre de l'alphabet ?

3° Quel calcul proposez vous pour obtenir à partir de y' un entier y permettant d'associer une lettre de l'alphabet ?

4° **Avec Excel ou LibreOfficeCalc** :

- la fonction MOD(a ; b) donne le reste de la division euclidienne de a par b.
- la fonction CAR ( ) associe à tout entier entre 97 et 122 sa lettre correspondante.

Faire apparaître y sur une nouvelle ligne puis le message codé sur la ligne suivante.

Partie B : le décodage

Celui qui reçoit le message n'a que y et la relation $y \equiv 19x+3$, il faut qu'il puisse retrouver x

1° Montrer que $19x+3 \equiv y\,[26]$ équivaut à $19x \equiv y-3\,[26]$

2° Déterminer un entier p tel que $19p \equiv 1\,[26]$

3° Que pouvez-vous dire alors de $19px$, x entier ? Justifiez

4° Montrer que $x \equiv 11y-33\,[26]$ et terminer le travail sur le tableur pour décoder le message.

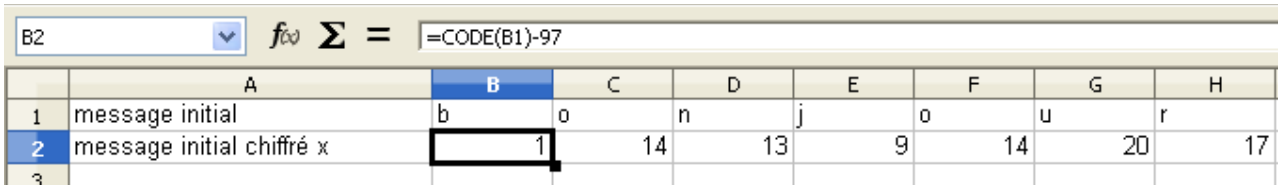
Partie C : un décodage toujours possible ?

Si deux valeurs distinctes x et x' donnent le même y le décodage devient impossible, un tel cas peut-il se produire ?

Le chiffrement affine :Eléments de correction

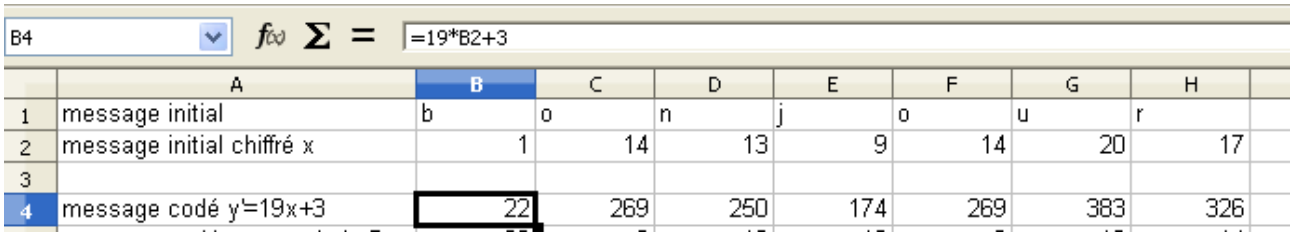
Partie A

Questions 1 et 2 :



B2 | =CODE(B1)-97

	A	B	C	D	E	F	G	H
1	message initial	b	o	n	j	o	u	r
2	message initial chiffré x	1	14	13	9	14	20	17
3								



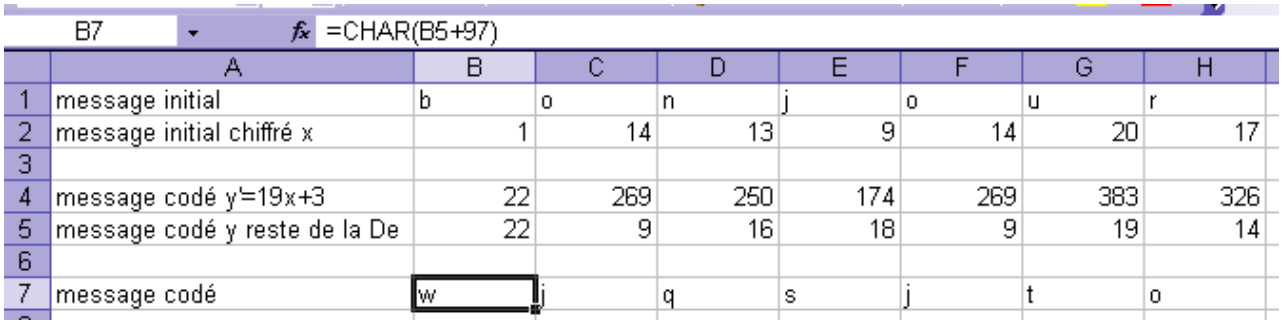
B4 | =19*B2+3

	A	B	C	D	E	F	G	H
1	message initial	b	o	n	j	o	u	r
2	message initial chiffré x	1	14	13	9	14	20	17
3								
4	message codé y'=19x+3	22	269	250	174	269	383	326

Question 3 : Quel calcul proposez vous pour obtenir à partir de y' un entier y permettant d'associer une lettre de l'alphabet ?

Nécessité d'utiliser le reste de y' dans la division euclidienne par 26 noté y
Pour définir y par rapport à x on introduit la notion de congruence :
$y \equiv 19x+3$ et on donne $a \equiv b[26]$ équivaut à $26|a-b$

Question 4 : Faire apparaître y sur une nouvelle ligne puis le message codé sur la ligne suivante.



B7 | =CHAR(B5+97)

	A	B	C	D	E	F	G	H
1	message initial	b	o	n	j	o	u	r
2	message initial chiffré x	1	14	13	9	14	20	17
3								
4	message codé y'=19x+3	22	269	250	174	269	383	326
5	message codé y reste de la De	22	9	16	18	9	19	14
6								
7	message codé	w	j	q	s	j	t	o

Partie B

Question 1: Montrer que $19x+3 \equiv y[26]$ équivaut à $19x \equiv y-3[26]$

$19x \equiv y-3[26]$ equivaut à $26|19x-(y-3)$ equivaut à $26|19x+3-y$ equivaut à $19x+3 \equiv y[26]$
On pourra généraliser $a \equiv b[n]$ et $a' \equiv b'[n]$ implique $a+b \equiv a'+b'[n]$

Question 2: Déterminer un entier p tel que $19p \equiv 1[26]$

le problème s'écrit : $19p = 26k+1$ c'est à dire $19p-26k=1$, le théorème de Bézout justifie de l'existence de p et l'algorithme d'Euclide permet de trouver $p = 11$.
Les élèves peuvent aussi trouver p par essais à la calculatrice.

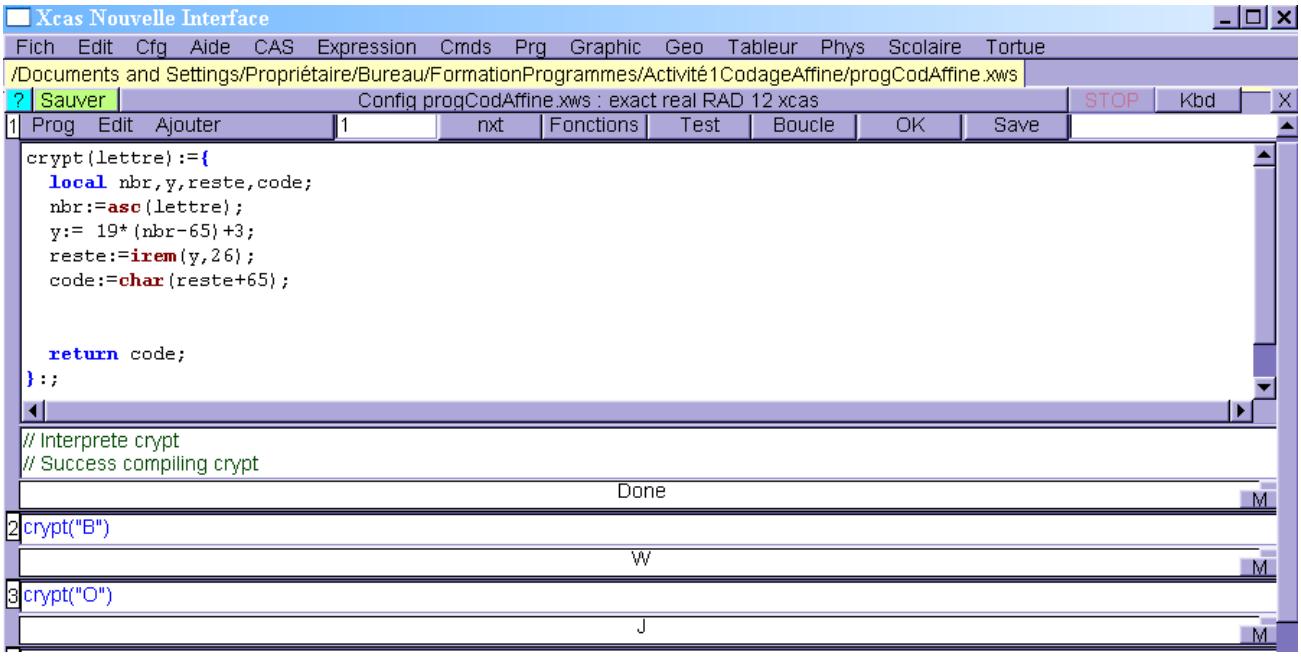
Question 3 : Que pouvez-vous dire alors de $19\,p\,x$, x entier ? Justifiez

- on a $26|(11\times19)-1$ donc pour tout entier x on a $26|x(11\times19)-x$ et $11\times19\,x\equiv x[26]$

On peut donner la propriété générale $a\equiv b[n]$ et $k\in\mathbb{Z}$ implique $a\,k\equiv k\,b[n]$

- on a alors $11\times19\,x\equiv11\,y-33[26]\equiv x[26]$

Prolongement on peut demander un algorithme de décodage aux élèves puis le programmer par exemple avec Xcas:
L'instruction : asc (« lettre ») numérise la lettre : entiers de 65 à 90 pour les majuscules
L'instruction : char (' nombre) donne le lettre associée au nombre
L'instruction : irem (a , b) donne le reste de la division euclidienne de a par b
Algorithme de codage :



Partie C

Question : Si deux valeurs distinctes x et x' donnent le même y le décodage devient impossible, un tel cas peut-il se produire ?

On a $y\equiv19\,x+3[26]\equiv19\,x'+3[26]$ donc $19(x-x')\equiv0[26]$ et $26|19(x-x')$ et $x\neq x'$

D'après le théorème de Gauss

$26|(x-x')$ or $-25\leqslant x-x'\leqslant25$ donc la division par $\{26\}$ n'est pas possible si $x\neq x'$

donc $x = x'$