Et cherchons l'entier k tel que $0 \leqslant x_0 + 26k \leqslant 25$

$-x_0 \leq 26k \leq 25 - x_0$

feuille n°4

avec k entier.

Prenons comme valeur de k l'entier k_0 compris entre $\frac{-x_0}{26}$ et $\frac{25-x_0}{26}$

D'où la valeur de a' = ...

Comme $a x \equiv y - b\ (26)$, on a par multiplication par a' : $a'ax \equiv a'(y-b)\ (26)$

or $a'a \equiv 1\ (26)$

$1x \equiv a'(y-b)\ (26)$

donc $x \equiv a'y - a'b\ (26)$ Posons $b' \equiv -a'b\ (26)$ avec $0 \leqslant b' \leqslant 25$, on obtient :

$x \equiv a'y + b'\ (26) \equiv g(y)\ (26)$

d'où **la clé de décodage est le couple d'entiers (a' ; b')**

b) Exemple : **Décoder le message suivant avec comme clé de codage (17 , 0) :** a = ... et b = ...

NRTKRXLLREP

lettre en clair	rang x	$a'y + b' \equiv x\ (26)$	rang y	lettre à décoder
				N
				R
				T
				K
				R
				X
				L
				L
				R
				E
				P

c) Comment décoder un message dont ne connait pas la clé de codage :

Soit le message suivant : **YMQMGGKAMMGNNELGMYZMN**

On sait qu'il est codé à l'aide d'une transformation affine . On sait que dans la langue française , **la lettre la plus fréquente est le E suivi de S .**

Donc comme **M apparait 6 fois suivi du G qui apparait 4 fois .** On suppose donc que **M correspond à E** et **G correspond à S .**

On écrit alors une **transformation affine** $x \to ax + b$ qui permet de **passer de E à M** et **de S à G .** Ce qui va permettre de trouver une clé de codage (a , b) , puis une clé de décodage (a' , b') en résolvant un système .

lettre	Rang x	$ax + b \equiv y\ (26)$	y	Lettre codée
E	4	$4a + b \equiv 12\ (26)$	12	M
S	18	$18a + b \equiv 6\ (26$	6	G

Résolution du système avec des congruences : $\begin{cases} 4a + b \equiv 12\ (26) & (2) \\ 18a + b \equiv 6\ (26) & (1) \end{cases}$

① * Montrer que $14a \equiv 20\ (26)$ puis que $7a \equiv 10\ (26)$

② * Déterminer u_0 et v_0 2 entiers tels que $7u_0 + 13v_0 = 1$, en déduire une solution particulière (x_0, y_0) de l'équation diophantienne $7x + 13y = 10$ puis la résoudre .

③ * En déduire que $a = 7$ ou $a = 20$

④ * Trouver alors la clé de codage (a , b) puis celle de décodage (a' , b') et décrypter le message initial .

c) comment décoder un message dont on ne connaît pas la clé de codage

résolution du système $\begin{cases} 4a+b \equiv 12\ (26) & (2) \\ 18a+b \equiv 6\ (26) & (1) \end{cases}$ $\times(-1)$

(1) $\oplus$ $-4a-b \equiv -12\ (26)$
$18a+b \equiv 6\ (26)$
$14a \equiv -6\ (26)$ or $-6 = -1\times 26 + 20$ où $0 \leq 20 < 26$
donc $-6 \equiv 20\ (26)$

donc $\boxed{14a \equiv 20\ (26)}$

donc $14a = 20 + 26q$ $\div 2$

$7a = 10 + 13q$

donc $\boxed{7a \equiv 10\ (13)}$

(2) si $\boxed{u_0 = 2}$ et $\boxed{v_0 = -1}$ alors $7u_0 + 13v_0 = 7\times 2 + 13\times(-1) = 14 - 13 = 1$

comme $7u_0 + 13v_0 = 1$

$7\times(10u_0) + 13\times(10v_0) = 10$ $\times 10$

$7x_0 + 13y_0 = 10$ avec $x_0 = 10u_0 = 10\times 2 = 20$

et $y_0 = 10v_0 = 10\times(-1) = -10$

donc $(x_0, y_0) = (20; -10)$ est une solution particulière de l'équation $7x + 13y = 10$

d'où $\begin{cases} 7x + 13y = 10 \\ 7x_0 + 13y_0 = 10 \end{cases}$

donc $7x + 13y = 7x_0 + 13y_0$

$7x - 7x_0 = 13y_0 - 13y$

$\boxed{7(x - x_0) = 13(y_0 - y)}$

donc d'après le th de Gauss

7 divise $y_0 - y$

donc il existe un entier k tel que $\boxed{y_0 - y = 7k}$

$y_0 - 7k = y$ or $y_0 = -10$

donc $\boxed{y = -10 - 7k}$

donc 7 divise $13(y_0 - y)$

7 et 13 sont premiers entre eux

(les diviseurs $\oplus$ de 7 sont : 1, 7
les diviseurs $\oplus$ de 13 sont : 1, 13
donc PGCD(7; 13) = 1)

par substitution $7 \mid (x - x_0) = 13 \times 7k$

$(x - x_0) = 13k$

$x = x_0 + 13k$ avec $x_0 = 20$

$\boxed{x = 20 + 13k}$

Réciproquement : si $x = 20 + 13k$ et $y = -10 - 7k$ alors $7x + 13y = 7(20 + 13k) + 13(-10 - 7k)$

$= 140 + 91k - 130 - 91k$

$= 10$

donc les solutions de l'équation $7x + 13y = 10$ sont tous les couples (x, y) de la forme $\boxed{(20 + 13k; -10 - 7k)}$ où k entier

(3) on a $7a \equiv 10\ (13)$

$7a = 10 + 13q$

$7a - 13q = 10$

$7a + 13(-q) = 10$

donc $(a, -q)$ est une solution de l'equation $7x + 13y = 10$

avec $0 \leq a \leq 25 < 26$

donc $a = x = 20 + 13k$ et $-q = y = -10 - 7k$.

$0 \leq a \leq 25$

$0 \leq 20 + 13k \leq 25$

$-20 \leq 13k \leq 5$ $\quad \div 13$ possible

$\frac{-20}{13} \leq k \leq \frac{5}{13}$ avec k entier donc $k = -1$ ou $k = 0$

$-1,53 \qquad 0,38$

donc pour $k = -1$: $a = 20 + 13k = 20 - 13 = 7$ | pour $k = 0$: $a = 20 + 13k = 20$

(4) or le codage affine est exploitable (ssi) a et 26 sont premiers entre eux

or si $a = 20$: les diviseurs ⊕ de a : 1, (2) 4, 5, 10, 20

les diviseurs de 26 : 1, (2) 13, 26

donc $PGCD(20, 26) = 2 \neq 1$ donc $a = 20$ ne convient pas

si $a = 7$ et $PGCD(7, 26) = 1$ (les diviseurs ⊕ de 7 sont : (1) et 7 ; les diviseurs ⊕ de 26 sont (1) 2, 13, 26)

donc $a = 7$ convient car 7 et 26 sont premiers entre eux

comme $4a + b \equiv 12\ (26)$ (2)

on a $b \equiv 12 - 4a\ (26)$

$b \equiv 12 - 4 \times 7\ (26)$

$b \equiv 12 - 28\ (26)$

$b \equiv -16\ (26)$

or $-16 = -1 \times 26 + 10$ avec $0 \leq 10 < 26$

donc $-16 \equiv 10\ (26)$

donc $b \equiv 10\ (26)$

la clé de codage est donc $(a, b) = (7, 10)$

et la fonction de codage est $f(x) = 7x + 10 \equiv y\ (26)$

Décodage :

$7x \equiv y - 10\ (26)$

$\times a'$ $\quad 7a'x \equiv a'(y - 10)\ (26)$

Trouvons a' tel que $7a' \equiv 1\ (26)$ avec $0 \leq a' < 26$

$7a' \equiv 1 (26)$

$7a' = 1 + 26q$

$7a' - 26q = 1$

$7a' + 26(-q) = 1$

$(a', -q)$ solution de l'equation $\boxed{7x + 26y = 1}$

si $x_0 = -11$ et $y_0 = 3$ alors $7x_0 + 26y_0 = 7 \times (-11) + 26 \times 3$
$= -77 + 78 = 1$

donc $(x_0, y_0) = (-11, 3)$ est solution particuliere de $7x + 26y = 1$

$\begin{cases} 7x + 26y = 1 \\ 7x_0 + 26y_0 = 1 \end{cases}$ donc $7x + 26y = 7x_0 + 26y_0$

$7x - 7x_0 = 26y_0 - 26y$

$\boxed{7(x - x_0) = 26(y_0 - y)}$

7 divise $26(y_0 - y)$
or 7 et 26 sont premiers entre eux

donc d'après le th de Gauss
7 divise $y_0 - y$
donc il existe un entier k tel que $\boxed{y_0 - y = 7k}$

$y_0 - 7k = y$ avec $y_0 = 3$

donc $\boxed{y = 3 - 7k}$

par substitution $7(x - x_0) = 26 \times 7k$

$x - x_0 = 26k$

$x = x_0 + 26k$ avec $x_0 = -11$

$\boxed{x = -11 + 26k}$

Réciproquement: si $x = -11 + 26k$ et $y = 3 - 7k$ alors $7x + 26y = 7(-11 + 26k) + 26(3 - 7k)$
$= -77 + 182k + 78 - 182k$
$= 1$

donc les solutions de l'equation $\boxed{7x + 26y = 1}$ sont tous les couples (x, y) de la forme $\boxed{(-11 + 26k ; 3 - 7k)}$ où k entier

donc $a' = x$ et $-q = y$

$a' = -11 + 26k$ avec $0 \leq a' \leq 25 < 26$

donc $0 \leq -11 + 26k \leq 25$

$11 \leq 26k \leq 25 + 11$

$\frac{11}{26} \leq k \leq \frac{36}{26}$ avec k entier.

$\frac{11}{26}$ $\quad$ $\frac{22}{26}$

$0,42$ $\quad$ $1,38$

donc $\boxed{k = 1}$ et $\boxed{a' = -11 + 26k = -11 + 26 \times 1 = 15}$

(ou $7a' \equiv a'(y - 10) (26)$

$7 \times 15 \equiv 15 (y - 10) (26)$ avec $7 \times 15 = 105 \equiv 1 (26)$

$1x \equiv 15(y-10) \quad (26)$

$x \equiv 15y - 150 \quad (26)$ or $-150 = -6 \times 26 + 6 \; (26)$

$\boxed{-150 \equiv 6 \; (26)}$

$\boxed{x \equiv 15y + 6 \; (26)}$

$x \equiv g(y) \; (26)$ où $\boxed{g(y) = 15y + 6}$ fonction de décodage

et la clé de décodage est $\boxed{(a', b') = (15; 6)}$

lettre en clair	x	$g(y) = 15y+6 \equiv x(26)$	rang y	lettre à décoder
C	$x=2$	$15y+6 = 15\times24+6 = 366 = 14\times26+2 \equiv 2(26)$	$y=24$	Y
E	$x=4$	$15y+6 = 15\times12+6 = 186 = 7\times26+4 \equiv 4(26)$	$y=12$	M
M	$x=12$	$15y+6 = 246 \equiv 12(26)$	$y=16$	Φ
E	$x=4$	$15y+6 = 186 \equiv 4(26)$	$y=16$	M
S	$x=18$	$15y+6 = 96 \equiv 18(26)$	$y=6$	G
S	$x=18$	$15y+6 = 96 \equiv 18(26)$	$y=6$	G
A	$x=0$	$15y+6 = 156 \equiv 0(26)$	$y=10$	K
G	$x=6$	$15y+6 = 6 \; (26)$	$y=0$	A
E	$x=4$	$15y+6 = 186 \equiv 4(26)$	$y=12$	M
E	$x=4$	$15y+6 = 186 \equiv 4(26)$	$y=12$	M
S	$x=18$	$15y+6 = 96 \equiv 18(26)$	$y=6$	G
T	$x=19$	$15y+6 = 201 \equiv 19(26)$	$y=13$	N
T	$x=19$	$15y+6 = 201 \equiv 19(26)$	$y=13$	N
O	$x=14$	$15y+6 = 66 \equiv 14(26)$	$y=4$	E
P	$x=15$	$15y+6 = 171 \equiv 15(26)$	$y=11$	L
S	$x=18$	$15y+6 = 96 \equiv 18(26)$	$y=6$	G
E	$x=4$	$15y+6 = 186 \equiv 4(26)$	$y=12$	M
C	$x=2$	$15y+6 = 366 \equiv 2(26)$	$y=24$	Y
R	$x=17$	$15y+6 = 381 \equiv 17(26)$	$y=25$	Z
E	$x=4$	$15y+6 = 186 \equiv 4(26)$	$y=12$	M
T	$x=19$	$15y+6 = 201 \equiv 19(26)$	$y=13$	N