$x = (y - 11) \times \frac{1}{21} z \ [26]$

Inverse z de 21 module 26 :

$21 \times z = z \times 21 \equiv 1 \ [26]$

$21 z = 1 + 26 k'' \quad , k'' \in \mathbb{Z}$

$21 z + 26 \times (-k'') = 1$

$21 = 3 \times 7$

$26 = 2 \times 13$

$26 k'' + 1 = 2 \times 13 \times k'' + 1$

$21 z - 26 k'' = 1$

eq. diophantienne, avec pgcd $(21, 26) = 1$.

26 | 21	21 | 5	5 | 1
−21 | 1	−20 | 4	−5 | 5
5	1	0

$26 = 21 \times 1 + 5$

$5 = 26 - 21 \times 1$

$21 = 5 \times 4 + 1$

$21 = (26 - 21) \times 4 + 1$

$21 = 26 \times 4 - 21 \times 4 + 1$

$21 + 21 \times 4 - 26 \times 4 = 1$

$21 \times 5 + 26 \times (-4) = 1$

Donc $k'' = 4$ et $z = 5$.

Vérification : $5 \times 21 = 105 = 104 + 1 = 4 \times 26 + 1 \equiv 1 \ [26]$

La fonction de décodage est donc $x = (y - 11) \times 5 \ [26]$,

i.e $g(y) = 5y - 55 \ [26]$.

4.) Décoder

G	L	B
6	11	1
−25	0	−50
1	0	2
B	A	C

$5 \times 6 - 55 = -25 \equiv 1 \ [26]$

$5 \times 11 - 55 = 0 \equiv 0 \ [26]$

$5 \times 1 - 55 = -50 \equiv 2 \ [26]$

N° .../...

Q 7. 18

ne rien écrire dans la partie barrée

Partie A (E) $11x - 26y = 1$, $x, y \in \mathbb{Z}$.

1°) $11 \times (-7) - 26 \times (-3) = 1$ (E')

Donc $(-7, -3)$ est une solution particulière de (E).

2°) (E) $11 \times x - 26 \times y = 1$

(E') $11 \times (-7) - 26 \times (-3) = 1$

on soustrait membre à membre

$11(x+7) - 26(y+3) = 0$

$11(x+7) = 26(y+3)$ (*)

Donc $26 \mid 11(x+7)$.

Or 26 et 11 sont premiers entre eux, donc d'après le théorème de Gauss

$26 \mid x+7$

$\exists k \in \mathbb{Z}$: $x + 7 = 26k$

$x = -7 + 26k$.

Dans (*) :

$11(26k) = 26(y+3)$

$y + 3 = 11k$

$y = -3 + 11k$

$S = \{ (-7+26k ; -3+11k) ; k \in \mathbb{Z} \}$.

3°) $u = -7 + 26k$, $k \in \mathbb{Z}$,

$0 \leq -7 + 26k \leq 25$

$7 \leq 26k \leq 32$

donc $k = 1$, d'où $u = -7 + 26 = 19$

et par suite $v = -3 + 11k = -3 + 11 = 8$

Vérification : $11 \times 19 - 26 \times 8 = 209 - 208 = 1$

Donc $(u, v) = (19; 8)$.

N° .../...

Partie B

$f(x) = 11x + 8 \ [26]$

1°) $W \to 22$

$11 \times 22 + 8 = 250 \equiv 16 \ [26]$

$16 \to Q$

Donc W se code en Q.

2a°) Pq $11x \equiv j \ [26] \iff x \equiv 19j \ [26]$

($\Rightarrow$) $11x \equiv j \ [26]$ $\times 19$

$\Rightarrow 209x \equiv 19j \ [26]$

$\Rightarrow 208x + x \equiv 19j \ [26]$

$\Rightarrow x \equiv 19j - 208x \ [26]$

$\Rightarrow x \equiv 19j - 8 \times \underline{26} x \ [26]$

$\Rightarrow x \equiv 19j \ [26]$

($\Leftarrow$) $x \equiv 19j \ [26]$ $\times 11$

$\Rightarrow 11x \equiv 209j \ [26]$

$\Rightarrow 11x \equiv j + 208j \ [26]$

$\Rightarrow 11x \equiv j + 8 \times \underline{26} j \ [26]$

$\Rightarrow 11x \equiv j \ [26]$

2°b) $y \equiv 11x + 8 \ [26]$

$11x \equiv y - 8 \ [26]$

$x \equiv \frac{1}{11}(y-8) \ [26]$

Or $11 \times x \equiv 1 \ [26] \iff x \equiv 19 \times 1 \ [26]$

(inverse de 11 mod 26)

Donc 19 est l'inverse de 11 modulo 26.

Donc $x \equiv 19(y-8) \ [26]$

$x \equiv 19y - 152 \ [26]$

$x \equiv 19y - 22 \ [26]$

$(152 = \overbrace{5 \times 26}^{130} + 22)$

Il $g(x) \equiv 19y - 22 \ [26]$ est la fonction de décodage.

2a $\iff x \equiv 19(y-8) \ [26]$

$\iff x \equiv 19y - 152 \ [26]$

$\iff x \equiv 19y - 22 \ [26]$.

2°c) W → 22

$19 \times 22 - 22 = 396 = 15 \times 26 + 6 \equiv 6 \ [26]$

6 → G

Donc W se décode en G.

(Non demandé : Vérification. G → 6

$11 \times 6 + 8 = 74 = 2 \times 26 + 22 \equiv 22 \ [26]$

22 → W (juste))

Ex 7.19 "petit théorème" de Fermat

Th : p premier, $a \in \mathbb{N}$.

Si $p \nmid a$, alors $p \mid a^{p-1} - 1$

Soient p premier, $a \in \mathbb{N}$ tq $p \nmid a$.

1°) $\forall k \in [\![1; p-1]\!]$, on note r_k : $ka \equiv r_k \ [p]$ et $0 \leq r_k \leq p-1$.

1a) Par l'absurde, supposons $r_k = 0$

$\exists k \in [\![1; p-1]\!]$: $ka \equiv 0 \ [p]$

$\exists k \in [\![1; p-1]\!]$: $p \mid ka$

Comme $p \nmid a$ (hypothèse), $p \mid k$ (th. Gauss). Or $k \leq p-1$, contradiction.

∥ Donc $\forall k \in [\![1; p-1]\!]$, $r_k \neq 0$

1°b) Soient $k, k' \in [\![1; p-1]\!]$ tq $r_k = r_{k'}$. On a $ka \equiv r_k \ [p]$ et $k'a \equiv r_{k'} \ [p]$.

Alors $ka \equiv k'a \ [p]$, i.e. $(k-k')a \equiv 0 \ [p]$

Donc • $k = k'$ (i.e. $k - k' = 0$)

ou bien • $a = 0$ (cas trivial)

ou bien • $p \mid (k-k')a$, et comme $p \nmid a$, $p \mid (k-k')$ (⇔ $p \mid a(k-k')$ or $p \nmid a$, donc (Gauss) $p \mid (k-k')$).

Or $k \leq p-1$

$k' \geq 1 \Rightarrow -k' \leq -1$

$k - k' \leq p-2 < p$, contradiction.

∥ Donc $k = k'$.

Ainsi les restes r_k, $k \in [\![1; p-1]\!]$ sont tous distincts

Comme $\#\{r_k \mid k \in [\![1; p-1]\!]\} = p-1$,

$r_k \in [\![1; p-1]\!]$, ($r_k = 0$ exclu car $\nu_p(a) = 0$)

et $\#[\![1; p-1]\!] = p-1$

$\Vert$ on a bien $\{r_1; r_2; \dots r_{p-1}\} = \{1; 2; \dots; p-1\}$.

1.c) On a : $\forall k \in [\![1, p-1]\!]$, $ka \equiv r_k \ [p]$

En multipliant membre à membre ces $(p-1)$ égalités, il vient :

$(1 \times 2 \times 3 \times \dots \times (p-1))\, a^{p-1} \equiv (r_1 \times r_2 \times \dots \times r_{p-1}) \ [p]$

$\Vert$ $(p-1)!\ a^{p-1} \equiv (p-1)! \ [p]$ (question 1.b)

2°) 1ère méthode : En multipliant membre à membre par l'inverse de $(p-1)!$ modulo p, il vient :

$a^{p-1} \equiv 1 \ [p]$ i.e. $a^{p-1} - 1 \equiv 0 \ [p]$, i.e. $p \mid (a^{p-1} - 1)$

2ème méthode : $(p-1)!\ a^{p-1} \equiv (p-1)! \ [p]$

$\Leftrightarrow (p-1)!\ (a^{p-1} - 1) \equiv 0 \ [p]$

$\Leftrightarrow p \mid (p-1)!\ (a^{p-1} - 1)$

Or $p \nmid (p-1)!$, car il ne figure pas dans la décomposition en facteurs premiers des entiers inférieurs à $p-1$, étant plus grand que ces nombres.

Donc $p \mid (a^{p-1} - 1)$ (th. de Gauss) Donc $a^{p-1} - 1 \equiv 0 \ [p]$

$\Rightarrow a^{p-1} \equiv 1 \ [p] \Rightarrow a^p \equiv a \ [p]$

3°) $\sum_{k=0}^{p-2} 2^k$ est la somme des termes d'une suite géométrique de raison 2.

$$\sum_{k=0}^{p-2} 2^k = \frac{1 - 2^{p-1}}{1-2} = \frac{1-2^{p-1}}{-1} = 2^{p-1} - 1.$$

Or p premier, $p \geq 3$. Donc $p \neq 2$.

D'après le petit théorème de Fermat, $p \mid 2^{p-1} - 1$,

i.e. $p \mid \sum_{k=0}^{p-2} 2^k$.