CORRIGÉ 93 page 137

Je ne me suis pas relu, je dois partir.
En général, sans relecture, il y a toujours au moins une coquille.
N'hésitez pas à m'écrire si vous en voyez une.

① La fonction de chiffrement est $f : \begin{array}{ccc} [\![0;34]\!] & \to & [\![0;34]\!] \\ x & \mapsto & y \equiv 10x+3\ [35] \end{array}$.

a) Soit $(x;y) \in [\![0;34]\!]^2$.
$y \equiv 10x+3\ [35] \iff \exists k \in \mathbb{Z}, y = 10x+3+35k \iff \exists k \in \mathbb{Z}, y-3 = 10x+35k$

b) Soit $(x;y;k) \in [\![0;34]\!]^2 \times \mathbb{Z}$.
L'équation $y-3 = 10x+35k$ admet au moins une seule solution si, et seulement si, $y-3$ est un multiple de PGCD(10;35)=5, donc si, et seulement si, $y \equiv 3\ [5]$

c) Contrairement à ce que j'ai dit à la fin du cours du 06/02/2024, la fonction de chiffrement est bien définie.

En effet, soit $x \in [\![0;34]\!]$.
$10x+3$ est bien sûr un unique nombre dans $[\![3;343]\!]$.
Il existe une infinité de nombres entiers y congrus à $10x+3$ modulo 35, et dans cette infinité, l'écart entre deux nombres successifs étant de 35, il en existe un (et un seul) dans $[\![0;34]\!]$.
Donc la fonction de chiffrement est bien définie, c'est-à-dire que l'image y de x existe quelle que soit la valeur de x dans $[\![0;34]\!]$; cette image est unique (ce qui fait que la fonction est bien une fonction), et cette image est bien dans $[\![0;34]\!]$.

Soit $y \in [\![0;34]\!]$. Deux cas sont possibles:

1er cas : $y \equiv 3\ [5]$. Alors il existe $x \in [\![0;34]\!]$ tel que $y \equiv 10x+3\ [35]$, autrement dit y admet un antécédent par la fonction de chiffrement.

2nd cas : $y \not\equiv 3\ [5]$. Alors y n'admet pas d'antécédent par la fonction de chiffrement. On a codé les 26 lettres et les accents par des nombres entiers dans $[\![0;34]\!]$. Si, par exemple, le caractère d est codé par le nombre 4 (qui est bien dans $[\![0;34]\!]$), alors, comme $4 \not\equiv 3\ [5]$, alors ce caractère n'est jamais présent dans le texte codé (le texte renvoyé par la fonction de chiffrement). En fait, les 35 caractères (avant chiffrement) sont codés sur seulement 7 caractères (qui sont ceux associés aux nombres 3; 8; 13; 18; 23; 28 et 33). Donc un caractère en sortie peut provenir de plusieurs caractère en entrée. En conclusion, il est possible de coder un texte avec cette fonction de chiffrement, mais il n'existe aucune fonction de déchiffrement, ce qui la rend inopérante.

② La fonction de chiffrement est $g : \begin{array}{ccc} [\![0;34]\!] & \to & [\![0;34]\!] \\ x & \mapsto & y \equiv 8x+5\ [35] \end{array}$.

a) PGCD(8;35)=1 donc, d'après le théorème de Bézout, il existe $(a;b) \in \mathbb{Z}^2$ tel que $8a+35b = 1$, donc (en prenant les deux membres modulo 35) il existe $a \in \mathbb{Z}$ tel que $8a \equiv 1\ [35]$.

Pour trouver un tel nombre a, utilisons l'algorithme d'Euclide étendu:

$35 = 4 \times 8 + 3$ donc $3 = 35 - 4 \times 8$

$8 = 2 \times 3 + 2$ donc $2 = 8 - 2 \times (35 - 4 \times 8) = -2 \times 35 + 9 \times 8$

$3 = 1 \times 2 + 1$ donc $1 = 3 - 2 = 35 - 4 \times 8 - (-2 \times 35 + 9 \times 8) = 3 \times 35 - 13 \times 8$

Finalement $8 \times (-13) \equiv 1\ [35]$ donc $a = -13$ convient.

b) Soit $(x;y) \in [\![0;34]\!]^2$. $y \equiv 8x+5\ [35] \implies 8x \equiv y-5\ [35] \implies 8x \times (-13) \equiv -13(y-5)\ [35] \implies 1 \times x \equiv -13y+65\ [35] \implies x \equiv 22y+30\ [35]$

où l'on a utilisé $8 \times (-13) = 1[35]$ et $-13 \equiv 22\ [35]$ et $65 \equiv 30\ [35]$

Pour $y \in [\![0; 34]\!]$, il existe un seul $x \in [\![0; 34]\!]$ tel que $x \equiv 22y + 30\ [35]$.

Réciproquement, soit $(x; y) \in [\![0; 34]\!]^2$ tel que $x \equiv 22y + 30\ [35]$.

Alors $8x + 5 \equiv 8(22y + 30) + 5\ [35]$ donc $8x + 5 \equiv 176y + 245\ [35]$ donc $8x + 5 \equiv y\ [35]$ car $176 \equiv 1\ [35]$ et $[245 \equiv 0\ [35]$

La fonction de décodage est donc h : $\begin{array}{ccc} [\![0; 34]\!] & \to & [\![0; 34]\!] \\ y & \mapsto & x \equiv 22y + 30\ [35] \end{array}$

c) L'entier chiffré par 9 est congru à $22 \times 9 + 30 = 228$ modulo 35 et il est dans $[\![0; 34]\!]$, c'est donc 18.