CORRECTION PARTIEL

EXERCICE 1

① • $8 = 2^3$ donc on peut convertir chiffre par chiffre (groupes de 3 bits).

$(1)_8 = (1)_2$
$(2)_8 = (10)_2$
$(5)_8 = (101)_2$
$\Rightarrow (125)_8 = (1010101)_2$

• $n = 5\times 8^0 + 2\times 8^1 + 1\times 8^2 = (85)_{10}$.

②

1	11	12	12
− +1	1+0	2+1	5
0	7	7	5

$(12)_8 - (5)_8 = (10)_{10} - (5)_{10} = (5)_{10} = (5)_8$.
$(12)_8 - (3)_8 = (10)_{10} - (3)_{10} = (7)_{10} = (7)_8$.
$(11)_8 - (2)_8 = (9)_{10} - (2)_{10} = (7)_{10} = (7)_8$.

③ $16 \mid n \iff 8 \mid n$ et $2 \mid \frac{n}{8}$
$\iff$ le dernier chiffre de n en base 8 est 0 et l'avant-dernier chiffre de n en base 8 est 0, 2, 4 ou 6.

EXERCICE 2

①

$$\begin{pmatrix} 1 & 0 & 47 \\ 0 & 1 & 14 \\ 1 & -3 & 5 \\ -2 & 7 & 4 \\ \boxed{3} & \boxed{-10} & \boxed{1} \\ \times & \times & 0 \end{pmatrix} \begin{matrix} \\ \\ L_1 - 3L_2 \\ L_2 - 2L_3 \\ L_3 - 1L_4 \\ L_4 - 4L_5 \end{matrix}$$

$47 = 14\times 3 + 5$
$14 = 5\times 2 + 4$
$5 = 4\times 1 + \boxed{1}$
$4 = 1\times 4 + 0$

L'algorithme d'Euclide étendu donne $d = PGCD(47,14) = 1$ et une relation de Bézout $47\times 3 + 14\times(-10) = 1$.

② D'après ①: $47\times 3 + 14\times(-10) = 1$

$\Rightarrow 47\times 9 + 14\times(-30) = 3$

Ainsi l'équation $47x + 14y = 3$ a pour solution particulière $(9,-30)$, donc d'après le cours l'ensemble de ses solutions est

$\mathcal{S} = \{(9+14k, -30-47k),\ k\in\mathbb{Z}\}$.

③ Comme $PGCD(47,14) = 1$, le théorème des restes chinois assure que l'ensemble des solutions de ce système est une unique classe de congruence modulo $47\times 14 = 658$. Cherchons une solution particulière x_0.

On veut $x_0 = 2+47k = 3+14\ell$ pour $k,\ell\in\mathbb{Z}$ à trouver.

$\Rightarrow 47k - 14\ell = 1$.

D'après ①: $(k,\ell) = (3,10)$ convient, ainsi

$x_0 = 2+47\times 3 = 3+14\times 10 = 143$ est solution particulière du système.

Conclusion : l'ensemble des solutions est $\{143+658k,\ k\in\mathbb{Z}\}$.

EXERCICE 5

Dans cet exercice, on note (E_n) l'équation $13x + 5y = n$.

① $(4, -1)$ est solution évidente de (E_{47}), et $PGCD(13,5) = 1$ (les deux nombres sont premiers) donc d'après le cours l'ensemble des solutions de (E_{47}) est $\{(4-5k, -1+13k),\ k \in \mathbb{Z}\}$.

② Je peux payer sans rendre de monnaie si et seulement si (E_{47}) admet une solution $(x,y) \in \underline{\mathbb{N}^2}$. (je donne alors x pièces de 13 et y pièces de 5).
Soit $(x,y) \in \underline{\mathbb{Z}^2}$ une solution de (E_{47}), d'après ① $\exists\, k \in \mathbb{Z}$ tel que $\begin{cases} x = 4 - 5k \\ y = -1 + 13k \end{cases}$.
Ainsi $x \geqslant 0 \iff k \leqslant \frac{4}{5} \iff k \leqslant 0$,
et $y \geqslant 0 \iff k \geqslant \frac{1}{13} \iff k \geqslant 1$.
Par conséquent soit x soit y est strictement négatif.
Il est impossible de payer 47 sans rendu de monnaie.

③ $49 = 13 \times 3 + 5 \times 2$ donc je peux payer 49 <u>sans</u> rendu de monnaie, en donnant 3 pièces de 13 et 2 pièces de 5.

④ $16 = 13 \times 2 + 5 \times (-2)$ donc je peux payer 16 <u>avec</u> rendu de monnaie, en donnant 2 pièces de 13 et on me rend 2 pièces de 5.

⑤ Soit $n \in \mathbb{N}$, et soit $(x_n, y_n) \in \mathbb{Z}^2$ une solution de (E_n) (qui existe car $PGCD(13,5) = 1 \mid n$), alors l'ensemble des solutions de (E_n) est $\{(x_n - 5k,\ y_n + 13k),\ k \in \mathbb{Z}\}$.
$\{x_n - 5k,\ k \in \mathbb{Z}\}$ est une classe de congruence modulo 5 donc possède un unique représentant dans $\{0,1,2,3,4\}$,
ce qui répond à la question.

⑥ 48, 49, 50 et 51 peuvent être payés sans rendu de monnaie, comme suit :

$$\begin{cases} 48 = 13\times 1 + 5\times 7 \\ 49 = 13\times 3 + 5\times 2 \quad \text{(question ③)} \\ 50 = 13\times 0 + 5\times 10 \\ 51 = 13\times 2 + 5\times 5 \end{cases}$$

Soit $n \geqslant 52$, d'après ⑤ il existe $(x,y) \in \mathbb{Z}^2$ tel que $13x + 5y = n$ et $0 < x \leq 4$.

$$\Rightarrow 5y = n - 13x \geqslant 52 - 13\times 4 = 0.$$

On a donc $x \geqslant 0$ et $y \geqslant 0$: n peut être payé sans rendu de monnaie.

EXERCICE 6

① $1823 \equiv 23 \equiv 5 \ [18]$ donc on cherche un représentant de la classe de 5^{242} modulo 18 qui soit entre 0 et 17.

→ Méthode 1 : Exponentiation rapide.

res	$\overline{a}$	$\overline{n}$
$\overline{1}$	$\overline{5}$	$242 = 2\times 121 + 0$
$\overline{1}$	$\overline{5}^2 = \overline{7}$	$121 = 2\times 60 + 1$
$\overline{1}\times\overline{7} = \overline{7}$	$\overline{7}^2 = \overline{13}$	$60 = 2\times 30 + 0$
$\overline{7}$	$\overline{13}^2 = \overline{7}$	$30 = 2\times 15 + 0$
$\overline{7}$	$\overline{7}^2 = \overline{13}$	$15 = 2\times 7 + 1$
$\overline{7}\times\overline{13} = \overline{1}$	$\overline{13}^2 = \overline{7}$	$7 = 2\times 3 + 1$
$\overline{1}\times\overline{7} = \overline{7}$	$\overline{7}^2 = \overline{13}$	$3 = 2\times 1 + 1$
$\overline{7}\times\overline{13} = \overline{1}$	$\overline{13}^2 = \overline{7}$	$1 = 2\times 0 + 1$
$\overline{1}\times\overline{7} = \boxed{\overline{7}}$	$\times$	0

$\Rightarrow \overline{1823}^{242} = \overline{7}$.

→ Méthode 2 : Théorème de Lagrange / Euler-Fermat.

On a $\varphi(18) = 6$ (cf. question ② à suivre)

donc d'après le théorème d'Euler-Fermat,

pour tout $a \in \mathbb{Z}$ premier avec 18 : $a^{\varphi(18)} = a^6 \equiv 1 \ [18]$.

Ici $\text{PGCD}(5,18) = 1$ donc le théorème s'applique : $\overline{5}^6 = \overline{1}$.

Comme $242 = 6\times 40 + 2$, $\overline{5}^{242} = \underbrace{(\overline{5}^6)^{40}}_{=\overline{1}} \times \overline{5}^2 = \overline{5}^2 = \boxed{\overline{7}}$.

② D'après le cours, $\overline{a} \in (\mathbb{Z}/18\mathbb{Z})^* \iff \text{PGCD}(a,18) = 1$.

on trouve $(\mathbb{Z}/18\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$

(et $\varphi(18) = |(\mathbb{Z}/18\mathbb{Z})^*| = 6$).

③ · Méthode 1 : Tout croyer à la main (18 calculs).

· Méthode 2 : Vu en TD.

$\overline{5}x = \overline{3} \iff 5x \equiv 3 \ [18]$

$\iff \exists y \in \mathbb{Z} \mid 5x = 3 + 18y$.

Cherchons les solutions entières de (E) : $5x - 18y = 3$.

$(-3, -1)$ est solution évidente donc l'ensemble des solutions est $\{(-3+18k, -1+5k), k \in \mathbb{Z}\}$

(en effet $PGCD(5,18) = 1$).

Ainsi $5x \equiv 3 \ [18]$ si et seulement si x est de la forme $-3+18k$ où $k \in \mathbb{Z}$. L'unique solution de $\overline{5}x = \overline{3}$ dans $\mathbb{Z}/18\mathbb{Z}$ est donc $-\overline{3} = \boxed{\overline{15}}$.

· Méthode 3 : Inverse ($\approx$ Méthode 2).

On a vu en ② que $\overline{5} \in (\mathbb{Z}/18\mathbb{Z})^*$.

Ainsi $\overline{5}x = \overline{3} \iff x = \overline{3} \times \overline{5}^{-1}$. Il reste à calculer l'inverse de $\overline{5}$ dans $(\mathbb{Z}/18\mathbb{Z})^*$, ce qui se fait à l'aide d'une relation de Bézout entre 5 et 18 :

$5 \times (-7) + 18 \times 2 = 1$

$\Rightarrow \overline{5} \times (-\overline{7}) = \overline{1}$

$\Rightarrow -\overline{7} = \overline{5}^{-1}$

L'unique solution de $\overline{5}x = \overline{3}$ est donc $x = \overline{3} \times (-\overline{7})$

$= -\overline{21} = \boxed{\overline{15}}$.