Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2023/2024.

Corrigé du contrôle terminal d'arithmétique et de cryptographie

Exercice 1.

$\mathbb{Z}a \subset \mathbb{Z}b$ donc $b \mid a$.
$a, b \in \mathbb{N}$, $a \neq 0$ et $b \mid a$ donc $b \leqslant a$.

Exercice 2.

$n \in \mathbb{N}$ et n est pair donc il existe $k \in \mathbb{N}$ tel que $n = 2k$.
$7^n = 7^{2k} = (7^2)^k = 49^k$ donc $7^n = 49^k$.
$2^n = 2^{2k} = (2^2)^k = 4^k$ donc $2^n = 4^k$.
$45 \mid 45$ donc $45 \mid 49 - 4$ donc $49 \equiv 4\ [45]$.
$49 \equiv 4\ [45]$ et $k \in \mathbb{N}$ donc $49^k \equiv 4^k\ [45]$.
$49^k \equiv 4^k\ [45]$ donc $7^n \equiv 2^n\ [45]$ donc $45 \mid 7^n - 2^n$.

Exercice 3.

- 1re solution.
  Soit $x \in \mathbb{Z}$. On suppose que $x \mid 9n + 8$ et $x \mid 6n + 5$.
  $x \mid 9n + 8$ donc $x \mid 2(9n + 8)$ donc $x \mid 18n + 16$.
  $x \mid 6n + 5$ donc $x \mid 3(6n + 5)$ donc $x \mid 18n + 15$.
  $x \mid 18n + 16$ et $x \mid 18n + 15$ donc $x \mid (18n + 16) - (18n + 15)$ donc $x \mid 1$.
  $x \mid 1$ donc $x = -1$ ou $x = 1$.

- 2de solution.

  * Vérifions que $\mathrm{Div}(9n + 8) \cap \mathrm{Div}(6n + 5) \subset \{-1, 1\}$.
    Soit $x \in \mathrm{Div}(9n + 8) \cap \mathrm{Div}(6n + 5)$.
    $x \in \mathrm{Div}(9n + 8) \cap \mathrm{Div}(6n + 5)$ donc $x \in \mathrm{Div}(9n + 8)$ et $x \in \mathrm{Div}(6n + 5)$.
    $x \in \mathrm{Div}(9n + 8)$ donc $x \mid 9n + 8$.
    $x \in \mathrm{Div}(6n + 5)$ donc $x \mid 6n + 5$.
    $x \mid 9n + 8$ donc $x \mid 2(9n + 8)$ donc $x \mid 18n + 16$.
    $x \mid 6n + 5$ donc $x \mid 3(6n + 5)$ donc $x \mid 18n + 15$.
    $x \mid 18n + 16$ et $x \mid 18n + 15$ donc $x \mid (18n + 16) - (18n + 15)$ donc $x \mid 1$.
    $x \mid 1$ donc $x \in \mathrm{Div}(1)$ donc $x \in \{-1, 1\}$.

  * Concluons.
    $\mathrm{Div}(9n + 8) \cap \mathrm{Div}(6n + 5) \subset \{-1, 1\}$ donc $9n + 8$ et $6n + 5$ sont premiers entre eux.

Exercice 4.

A] 1) • 1re solution.
  n est pair donc $2 \mid n$.
  $2 \mid n$, $2 \mid 2$, $2 \neq -1$ et $2 \neq 1$ donc n et 2 ne sont pas premiers entre eux.

- 2^{de} solution.
  n est pair donc $2 \mid n$ donc $2 \in \text{Div}(n)$.
  $2 \in \text{Div}(n)$ et $2 \in \text{Div}(2)$ donc $2 \in \text{Div}(n) \cap \text{Div}(2)$.
  $2 \neq -1$ et $2 \neq 1$ donc $2 \notin \{-1, 1\}$.
  $2 \in \text{Div}(n) \cap \text{Div}(2)$ et $2 \notin \{-1, 1\}$ donc $\text{Div}(n) \cap \text{Div}(2) \neq \{-1, 1\}$.
  $\text{Div}(n) \cap \text{Div}(2) \neq \{-1, 1\}$ donc n et 2 ne sont pas premiers entre eux.

2) - 1^{re} solution.
  n est pair donc $2 \mid n$.
  $2 \mid n$ et $2 \mid 2$ donc $2 \mid n + 2$.
  $2 \mid n$, $2 \mid n + 2$, $2 \neq -1$ et $2 \neq 1$ donc n et $n + 2$ ne sont pas premiers entre eux.

- 2^{de} solution.
  n est pair donc $2 \mid n$.
  $2 \mid n$ donc $2 \in \text{Div}(n)$.
  $2 \mid n$ et $2 \mid 2$ donc $2 \mid n + 2$ donc $2 \in \text{Div}(n + 2)$.
  $2 \in \text{Div}(n)$ et $2 \in \text{Div}(n + 2)$ donc $2 \in \text{Div}(n) \cap \text{Div}(n + 2)$.
  $2 \neq -1$ et $2 \neq 1$ donc $2 \notin \{-1, 1\}$.
  $2 \in \text{Div}(n) \cap \text{Div}(n + 2)$ et $2 \notin \{-1, 1\}$ donc $\text{Div}(n) \cap \text{Div}(n + 2) \neq \{-1, 1\}$.
  $\text{Div}(n) \cap \text{Div}(n + 2) \neq \{-1, 1\}$ donc n et $n + 2$ ne sont pas premiers entre eux.

B] 1) n est impair donc il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$.
  $1n + (-k)2 = 1$ donc n et 2 sont premiers entre eux.

2) - 1^{re} solution.
  Soit $x \in \mathbb{Z}$. On suppose que $x \mid n$ et $x \mid n + 2$.
  $x \mid n + 2$ et $x \mid n$ donc $x \mid (n + 2) - n$ donc $x \mid 2$.
  $x \mid n$, $x \mid 2$ et (d'après 1)) n et 2 sont premiers entre eux donc $x = -1$ ou $x = 1$.

- 2^{de} solution.

  * Vérifions que $\text{Div}(n) \cap \text{Div}(n + 2) \subset \{-1, 1\}$.
    Soit $x \in \text{Div}(n) \cap \text{Div}(n + 2)$.
    $x \in \text{Div}(n) \cap \text{Div}(n + 2)$ donc $x \in \text{Div}(n)$ et $x \in \text{Div}(n + 2)$.
    $x \in \text{Div}(n)$ donc $x \mid n$.
    $x \in \text{Div}(n + 2)$ donc $x \mid n + 2$.
    $x \mid n + 2$ et $x \mid n$ donc $x \mid (n + 2) - n$ donc $x \mid 2$ donc $x \in \text{Div}(2)$.
    $x \in \text{Div}(n)$ et $x \in \text{Div}(2)$ donc $x \in \text{Div}(n) \cap \text{Div}(2)$.
    Par 1) n et 2 sont premiers entre eux, donc $\text{Div}(n) \cap \text{Div}(2) = \{-1, 1\}$.
    D'où $x \in \{-1, 1\}$.

  * Concluons.
    $\text{Div}(n) \cap \text{Div}(n + 2) \subset \{-1, 1\}$ donc n et $n + 2$ sont premiers entre eux.

C] - * 2023 et $2023 + 1$ sont premiers entre eux donc 2023 et 2024 sont premiers entre eux.

  * 2024 et $2024 + 1$ sont premiers entre eux donc 2024 et 2025 sont premiers entre eux.

  * $2023 = 2 \times 1011 + 1$ donc 2023 est impair.
    2023 est impair donc (par B]2)) 2023 et $2023 + 2$ sont premiers entre eux.
    Ainsi 2023 et 2025 sont premiers entre eux.

- 2023 et 2024 sont premiers entre eux, 2023 et 2025 sont premiers entre eux, 2024 et 2025 sont premiers entre eux, donc 2023, 2024 et 2025 sont deux à deux premiers entre eux.

- $2023 \mid a$, $2024 \mid a$, $2025 \mid a$ et 2023, 2024 et 2025 sont deux à deux premiers entre eux donc $(2023 \times 2024 \times 2025) \mid a$.

Exercice 5.

1) Soit $x \in A + C$.
$x \in A + C$ donc il existe $a \in A$ et $c \in C$ tels que $x = a + c$.
$a \in A$ et $A \subset B$ donc $a \in B$.
$a \in B$ et $c \in C$ donc $a + c \in B + C$. D'où $x \in B + C$.

2) - 1^{re} solution.
$F \cap G \subset F$ donc (par 1)) $(F \cap G) + H \subset F + H$.
$F \cap G \subset G$ donc (par 1)) $(F \cap G) + H \subset G + H$.
$(F \cap G) + H \subset F + H$ et $(F \cap G) + H \subset G + H$ donc $(F \cap G) + H \subset (F + H) \cap (G + H)$.

   - 2^{de} solution.
Soit $x \in (F \cap G) + H$.
$x \in (F \cap G) + H$ donc il existe $y \in F \cap G$ et $h \in H$ tels que $x = y + h$.
$y \in F \cap G$ donc $y \in F$ et $y \in G$.
$y \in F$ et $h \in H$ donc $y + h \in F + H$. D'où $x \in F + H$.
$y \in G$ et $h \in H$ donc $y + h \in G + H$. D'où $x \in G + H$.
$x \in F + H$ et $x \in G + H$ donc $x \in (F + H) \cap (G + H)$.

Exercice 6.

1) Soit $z \in \mathbb{Z}$.
4 et 9 sont premiers entre eux donc il existe $x, y \in \mathbb{Z}$ tels que $x \times 4 + y \times 9 = z$.
$4x + 9y = z$ donc $f(x, y) = z$.

2) $f(9, 0) = 36$ et $f(0, 4) = 36$ donc $f(9, 0) = f(0, 4)$.
$9 \neq 0$ donc $(9, 0) \neq (0, 4)$.
$f(9, 0) = f(0, 4)$ et $(9, 0) \neq (0, 4)$ donc f n'est pas injective.