Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2022/2023.

Corrigé du contrôle terminal d'arithmétique et de cryptographie

Exercice 1.

$25 = 8 + 1 \times 17$ donc $25 \equiv 8$ [17]. $25 \equiv 8$ [17] et $n \in \mathbb{N}$ donc $25^n \equiv 8^n$ [17].
$25^n \equiv 8^n$ [17] donc $25^n + 2^{3n+4} \equiv 8^n + 2^{3n+4}$ [17].
$2^{3n+4} = 2^{3n} \times 2^4 = (2^3)^n \times 16 = 8^n \times 16$ donc $2^{3n+4} = 8^n \times 16$. D'où $8^n + 2^{3n+4} = 8^n + 8^n \times 16$.
$8^n + 8^n \times 16 = 8^n \times 1 + 8^n \times 16 = 8^n \times (1 + 16) = 8^n \times 17$ donc $8^n + 2^{3n+4} = 8^n \times 17$.
$8^n \times 17 \equiv 0$ [17] donc $8^n + 2^{3n+4} \equiv 0$ [17].
$25^n + 2^{3n+4} \equiv 8^n + 2^{3n+4}$ [17] et $8^n + 2^{3n+4} \equiv 0$ [17] donc $25^n + 2^{3n+4} \equiv 0$ [17] donc $17 \mid 25^n + 2^{3n+4}$.

Exercice 2.

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) • Montrons que $(F + H) \cup (G + H) \subset (F \cup G) + H$.
$F \subset F \cup G$ donc (par 1)) $F + H \subset (F \cup G) + H$.
$G \subset F \cup G$ donc (par 1)) $G + H \subset (F \cup G) + H$.
$F + H \subset (F \cup G) + H$ et $G + H \subset (F \cup G) + H$ donc $(F + H) \cup (G + H) \subset (F \cup G) + H$.

• Montrons que $(F \cup G) + H \subset (F + H) \cup (G + H)$.
Soit $y \in (F \cup G) + H$.
$y \in (F \cup G) + H$ donc il existe $x \in F \cup G$ et $h \in H$ tels que $y = x + h$.
$x \in F \cup G$ donc $x \in F$ ou $x \in G$. On distingue donc deux cas.
∗ On suppose $x \in F$.
$x \in F$ et $h \in H$ donc $x + h \in F + H$ donc $y \in F + H$.
$y \in F + H$ et $F + H \subset (F + H) \cup (G + H)$ donc $y \in (F + H) \cup (G + H)$.
∗ On suppose $x \in G$.
$x \in G$ et $h \in H$ donc $x + h \in G + H$ donc $y \in G + H$.
$y \in G + H$ et $G + H \subset (F + H) \cup (G + H)$ donc $y \in (F + H) \cup (G + H)$.
On en déduit que $y \in (F + H) \cup (G + H)$.

• Concluons.
$(F \cup G) + H \subset (F + H) \cup (G + H)$ et $(F + H) \cup (G + H) \subset (F \cup G) + H$ donc
$(F \cup G) + H = (F + H) \cup (G + H)$.

Exercice 3.

1) n est pair ou n est impair ; on distingue donc deux cas.

• On suppose n pair.
n est pair donc $2 \mid n$ donc $2 \mid (n + 1)n$ donc $2 \mid n(n + 1)$.

• On suppose n impair.
n est impair donc $n + 1$ est pair donc $2 \mid n + 1$ donc $2 \mid n(n + 1)$.

On en déduit que $2 \mid n(n+1)$.

2) Notons r le reste dans la division euclidienne de n par 3. Ainsi $n \equiv r\ [3]$.
$0 \leqslant r < |3|$ donc $r = 0$ ou $r = 1$ ou $r = 2$. On distingue donc trois cas.

- On suppose $r = 0$.
$r = 0$ donc le reste dans la division euclidienne de n par 3 vaut 0 donc $3 \mid n$.
$3 \mid n$ donc $3 \mid ((n+1)(2n+1))n$ donc $3 \mid n(n+1)(2n+1)$.

- On suppose $r = 1$.
$n \equiv r\ [3]$ et $r = 1$ donc $n \equiv 1\ [3]$ donc $2n \equiv 2 \times 1\ [3]$ donc $2n \equiv 2\ [3]$.
$2n \equiv 2\ [3]$ donc $2n + 1 \equiv 2 + 1\ [3]$ donc $2n + 1 \equiv 3\ [3]$.
$2n + 1 \equiv 3\ [3]$ et $3 \equiv 0\ [3]$ donc $2n + 1 \equiv 0\ [3]$ donc $3 \mid 2n + 1$.
$3 \mid 2n + 1$ donc $3 \mid (n(n+1))(2n+1)$ donc $3 \mid n(n+1)(2n+1)$.

- On suppose $r = 2$.
$n \equiv r\ [3]$ et $r = 2$ donc $n \equiv 2\ [3]$ donc $n + 1 \equiv 2 + 1\ [3]$ donc $n + 1 \equiv 3\ [3]$.
$n + 1 \equiv 3\ [3]$ et $3 \equiv 0\ [3]$ donc $n + 1 \equiv 0\ [3]$ donc $3 \mid n + 1$.
$3 \mid n + 1$ donc $3 \mid (n(2n+1))(n+1)$ donc $3 \mid n(n+1)(2n+1)$.

On en déduit que $3 \mid n(n+1)(2n+1)$.

3) Par 1), $2 \mid n(n+1)$. $2 \mid n(n+1)$ donc $2 \mid (2n+1)(n(n+1))$ donc $2 \mid n(n+1)(2n+1)$.
$2 \mid n(n+1)(2n+1)$, $3 \mid n(n+1)(2n+1)$, 2 et 3 sont premiers entre eux, donc $2 \times 3 \mid n(n+1)(2n+1)$.
D'où $6 \mid n(n+1)(2n+1)$.

Exercice 4.

- Montrons que $a = c$.

  * Montrons que $a \mid c$.
  $a \mid ab$ et $ab = cd$ donc $a \mid cd$. $a \mid cd$ et a est premier avec d donc $a \mid c$.

  * Montrons que $c \mid a$.
  $c \mid cd$ et $ab = cd$ donc $c \mid ab$. $c \mid ab$ et c est premier avec b donc $c \mid a$.

  * Concluons.
  $a \mid c$, $c \mid a$, $a \in \mathbb{N}$ et $c \in \mathbb{N}$ donc $a = c$.

- Montrons que $b = d$.
On propose deux preuves.

  1) Première preuve.
  Cette preuve est similaire à celle de $a = c$.

     * Montrons que $b \mid d$.
     $b \mid ab$ et $ab = cd$ donc $b \mid cd$. $b \mid cd$ et b est premier avec c donc $b \mid d$.

     * Montrons que $d \mid b$.

$d \mid cd$ et $ab = cd$ donc $d \mid ab$. $d \mid ab$ et d est premier avec a donc $d \mid b$.

∗ Concluons.
$b \mid d$, $d \mid b$, $b \in \mathbb{N}$ et $d \in \mathbb{N}$ donc $b = d$.

2) Seconde preuve.

On distingue deux cas.

∗ On suppose $c \neq 0$.
$ab = cd$ et $a = c$ donc $cb = cd$. $cb = cd$ et $c \neq 0$ donc $b = d$.

∗ On suppose $c = 0$.
— Montrons que $b = 1$.
b est premier avec c et $c = 0$ donc b est premier avec 0.
b est premier avec 0 donc $b = 1$ ou $b = -1$. Or $b \in \mathbb{N}$, donc $b = 1$.
— Montrons que $d = 1$.
$a = c$ et $c = 0$ donc $a = 0$.
d est premier avec a et $a = 0$ donc d est premier avec 0.
d est premier avec 0 donc $d = -1$ ou $d = 1$. Or $d \in \mathbb{N}$, donc $d = 1$.
— Concluons.
$b = 1$ et $d = 1$ donc $b = d$.

Exercice 5.

$\forall p \in \mathcal{P}$ $p \mid a$ donc $\forall p \in \mathcal{P}$ $p \in \mathrm{Div}(a)$ donc $\mathcal{P} \subset \mathrm{Div}(a)$.
$\mathcal{P}$ est infini et $\mathcal{P} \subset \mathrm{Div}(a)$ donc $\mathrm{Div}(a)$ est infini.
On sait que pour tout $x \in \mathbb{Z} \setminus \{0\}$ $\mathrm{Div}(x)$ est fini. $\mathrm{Div}(a)$ est infini donc $a = 0$.

Exercice 6.

1)

2) Commençons par justifier que $\mathbb{Z}(ab) \subset \mathbb{Z}a \cap \mathbb{Z}b$.
$a \mid ab$ donc $\mathbb{Z}(ab) \subset \mathbb{Z}a$.
$b \mid ab$ donc $\mathbb{Z}(ab) \subset \mathbb{Z}b$.
$\mathbb{Z}(ab) \subset \mathbb{Z}a$ et $\mathbb{Z}(ab) \subset \mathbb{Z}b$ donc $\mathbb{Z}(ab) \subset \mathbb{Z}a \cap \mathbb{Z}b$.

• Montrons i) $\Longrightarrow$ ii).
On suppose a et b premiers entre eux.

∗ Vérifions que $\mathbb{Z}a \cap \mathbb{Z}b \subset \mathbb{Z}(ab)$.
Soit $x \in \mathbb{Z}a \cap \mathbb{Z}b$.
$x \in \mathbb{Z}a \cap \mathbb{Z}b$ donc $x \in \mathbb{Z}a$ et $x \in \mathbb{Z}b$.
$x \in \mathbb{Z}a$ donc $a \mid x$.
$x \in \mathbb{Z}b$ donc $b \mid x$.
$a \mid x$, $b \mid x$, a et b sont premiers entre eux, donc $ab \mid x$.
$ab \mid x$ donc $x \in \mathbb{Z}(ab)$.

∗ Concluons.

$\mathbb{Z}a \cap \mathbb{Z}b \subset \mathbb{Z}(ab)$ et $\mathbb{Z}(ab) \subset \mathbb{Z}a \cap \mathbb{Z}b$ donc $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}(ab)$.

- Montrons ii) $\Longrightarrow$ i).
  On suppose que $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}(ab)$.
  Soit $x \in \mathbb{Z}$. On suppose que $x \mid a$ et $x \mid b$.
  $x \mid a$ donc il existe $a' \in \mathbb{Z}$ tel que $a = a'x$.
  $x \mid b$ donc il existe $b' \in \mathbb{Z}$ tel que $b = b'x$.
  On note $c = a'b'x$.
  $c = a'b'x$ et $a = a'x$ donc $c = b'a$ donc $c \in \mathbb{Z}a$.
  $c = a'b'x$ et $b = b'x$ donc $c = a'b$ donc $c \in \mathbb{Z}b$.
  $c \in \mathbb{Z}a$ et $c \in \mathbb{Z}b$ donc $c \in \mathbb{Z}a \cap \mathbb{Z}b$.
  $c \in \mathbb{Z}a \cap \mathbb{Z}b$ et $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}(ab)$ donc $c \in \mathbb{Z}(ab)$ donc $ab \mid c$.
  $ab \mid c$ donc $(ab)x \mid cx$.
  $cx = (a'b'x)x = (a'x)(b'x) = ab$ donc $cx = ab$.
  $(ab)x \mid cx$ et $cx = ab$ donc $(ab)x \mid ab$.
  $a \neq 0$ et $b \neq 0$ donc $ab \neq 0$.
  $(ab)x \mid (ab)1$ et $ab \neq 0$ donc $x \mid 1$.
  $x \mid 1$ donc $x = 1$ ou $x = -1$.