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

Corrigé du contrôle continu d'arithmétique et de cryptographie

Exercice 1.

On remarque que $m^2 + m = m(m+1)$.
On distingue deux cas : m pair et m impair.

- On suppose m pair.
  m est pair donc $m(m+1)$ est pair donc $m^2 + m$ est pair.

- On suppose m impair.
  m est impair donc $m+1$ est pair donc $m(m+1)$ est pair donc $m^2 + m$ est pair.

Exercice 2.

On propose deux solutions.

1) Première solution.
   On procède par récurrence.

   - Initialisation.
     $(a+1)^0 - a \times 0 - 1 = 1 - 0 - 1 = 0$. $a^2 \mid 0$ donc $a^2 \mid (a+1)^0 - a \times 0 - 1$.

   - Hérédité.
     Soit $n \in \mathbb{N}$. On suppose que $a^2 \mid (a+1)^n - an - 1$.
     $a^2 \mid (a+1)^n - an - 1$ donc $a^2 \mid (a+1)\Big((a+1)^n - an - 1\Big)$.
     $(a+1)\Big((a+1)^n - an - 1\Big) = (a+1)^{1+n} - a^2 n - a - an - 1 = (a+1)^{n+1} - a(n+1) - 1 - a^2 n$.
     $a^2 \mid (a+1)^{n+1} - a(n+1) - 1 - a^2 n$ et $a^2 \mid a^2 n$ donc $a^2 \mid \Big((a+1)^{n+1} - a(n+1) - 1 - a^2 n\Big) + a^2 n$
     donc $a^2 \mid (a+1)^{n+1} - a(n+1) - 1$.

2) Seconde solution.
   Soit $n \in \mathbb{N}$. On distingue trois cas : $n = 0$, $n = 1$ et $n \geqslant 2$.

   - On suppose $n = 0$.
     $(a+1)^n - an - 1 = (a+1)^0 - a \times 0 - 1 = 1 - 0 - 1 = 0$.
     $a^2 \mid 0$ donc $a^2 \mid (a+1)^n - an - 1$.

   - On suppose $n = 1$.
     $(a+1)^n - an - 1 = (a+1)^1 - a \times 1 - 1 = a + 1 - a - 1 = 0$.
     $a^2 \mid 0$ donc $a^2 \mid (a+1)^n - an - 1$.

   - On suppose $n \geqslant 2$.
     La formule du binôme de Newton donne $(a+1)^n = \displaystyle\sum_{k=0}^{n} C_n^k a^k 1^{n-k}$.
     Donc $(a+1)^n = \displaystyle\sum_{k=0}^{n} C_n^k a^k \times 1 = \sum_{k=0}^{n} C_n^k a^k$.

$n \geqslant 2$ donc $\sum_{k=0}^{n} C_n^k a^k = C_n^0 a^0 + C_n^1 a^1 + \sum_{k=2}^{n} C_n^k a^k = 1 \times 1 + na + \sum_{k=2}^{n} C_n^k a^k$ donc

$(a+1)^n = 1 + na + \sum_{k=2}^{n} C_n^k a^k$ donc $(a+1)^n - an - 1 = \sum_{k=2}^{n} C_n^k a^k$.

$\forall k \geqslant 2\ a^2 \mid a^k$ donc $\forall k \in \{2, \ldots, n\}\ a^2 \mid a^k$ donc $\forall k \in \{2, \ldots, n\}\ a^2 \mid C_n^k a^k$.

$\forall k \in \{2, \ldots, n\}\ a^2 \mid C_n^k a^k$ donc $a^2 \mid \sum_{k=2}^{n} C_n^k a^k$ donc $a^2 \mid (a+1)^n - an - 1$.

Exercice 3.

1) Soit $x \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$.
$x \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$ donc $x \in \mathrm{Div}(a)$ et $x \in \mathrm{Div}(b)$ donc $x \mid a$ et $x \mid b$.
$x \mid a$ et $x \mid b$ donc $x \mid a + b$ donc $x \in \mathrm{Div}(a+b)$.

2) On pose $a = 2$ et $b = -1$.
On a bien $a, b \in \mathbb{Z}$. On a bien $a \neq 0$ et $b \neq 0$.
$\mathrm{Div}(2) \cap \mathrm{Div}(-1) = \mathrm{Div}(2) \cap \mathrm{Div}(1) = \{-2, -1, 1, 2\} \cap \{-1, 1\} = \{-1, 1\} = \mathrm{Div}(1) = \mathrm{Div}(2 + (-1))$
donc $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a+b)$.

3) • Vérifions que i) $\Longrightarrow$ ii).
On suppose $a = 0$ ou $b = 0$.
Si $a = 0$, alors $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(0) \cap \mathrm{Div}(b) = \mathbb{Z} \cap \mathrm{Div}(b) = \mathrm{Div}(b) = \mathrm{Div}(0+b) = \mathrm{Div}(a+b)$.
Si $b = 0$, alors $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a) \cap \mathrm{Div}(0) = \mathrm{Div}(a) \cap Z = \mathrm{Div}(a) = \mathrm{Div}(a+0) = \mathrm{Div}(a+b)$.
Donc ii) est vraie.

• Montrons que ii) $\Longrightarrow$ i).
On suppose $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a+b)$.
$a + b \in \mathrm{Div}(a+b)$ donc $a + b \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$ donc $a + b \in \mathrm{Div}(a)$ donc $a + b \mid a$.
On distingue deux cas : $a = 0$ et $a \neq 0$.

∗ On suppose $a = 0$.
Dans ce cas i) est bien vraie.

∗ On suppose $a \neq 0$.
$a + b \in \mathbb{N}$, $a \in \mathbb{N}$, $a \neq 0$ et $a + b \mid a$ donc $a + b \leqslant a$.
$a + b \leqslant a$ donc $b \leqslant 0$. $b \leqslant 0$ et $b \in \mathbb{N}$ donc $b = 0$. Donc i) est bien vraie.

Exercice 4.

• $3^{3k} = (3^3)^k = 27^k$.
$27 = 1 + 2 \times 13$ donc $27 \equiv 1\ [13]$.
$k \in \mathbb{N}$ et $27 \equiv 1\ [13]$ donc $27^k \equiv 1^k\ [13]$ donc $3^{3k} \equiv 1\ [13]$.

• $5^{4\ell+2} = 5^{2(2\ell+1)} = (5^2)^{2\ell+1} = 25^{2\ell+1}$.
$25 = -1 + 2 \times 13$ donc $25 \equiv -1\ [13]$.
$2\ell + 1 \in \mathbb{N}$ et $25 \equiv -1\ [13]$ donc $25^{2\ell+1} \equiv (-1)^{2\ell+1}\ [13]$ donc $5^{4\ell+2} \equiv -1\ [13]$.

• $3^{3k} \equiv 1\ [13]$ et $5^{4\ell+2} \equiv -1\ [13]$ donc $3^{3k} + 5^{4\ell+2} \equiv 1 + (-1)\ [13]$ donc $3^{3k} + 5^{4\ell+2} \equiv 0\ [13]$.
$3^{3k} + 5^{4\ell+2} \equiv 0\ [13]$ donc $13 \mid 3^{3k} + 5^{4\ell+2}$.

Exercice 5.

- On suppose $a \geqslant 1$.
  On remarque que $a^2 - 1 = (a-1)a + (a-1)$.
  $a \geqslant 1$ donc $a - 1 \geqslant 0$.
  $a \geqslant 1$ donc $a \geqslant 0$ donc $|a| = a$.
  $a - 1 < a$ donc $a - 1 < |a|$.
  $a^2 - 1 = (a-1)a + (a-1)$ et $0 \leqslant a - 1 < |a|$ donc, dans la division euclidienne de $a^2 - 1$ par a, le quotient vaut $a - 1$ et le reste vaut $a - 1$.

- On suppose $a \leqslant -1$.
  On remarque que $a^2 - 1 = (a+1)a + (-a-1)$.
  $a \leqslant -1$ donc $-a - 1 \geqslant 0$.
  $a \leqslant -1$ donc $a \leqslant 0$ donc $|a| = -a$.
  $-a - 1 < -a$ donc $-a - 1 < |a|$.
  $a^2 - 1 = (a+1)a + (-a-1)$ et $0 \leqslant -a - 1 < |a|$ donc, dans la division euclidienne de $a^2 - 1$ par a, le quotient vaut $a + 1$ et le reste vaut $-a - 1$.

Exercice 6.

A] Vérifions ii) $\Longrightarrow$ i).
On suppose ii) vraie.
On distingue trois cas.

1) On suppose $m = \ell$ et $n = \ell$.
   $\ell \mid 2\ell$ donc $\ell \mid m + n$.
   $\ell \mid 2\ell$ donc $m \mid n + \ell$.
   $\ell \mid 2\ell$ donc $n \mid m + \ell$.
   Donc i) est vraie.

2) On suppose $m = \ell$ et $n = 2\ell$.
   $\ell \mid 3\ell$ donc $\ell \mid m + n$.
   $\ell \mid 3\ell$ donc $m \mid n + \ell$.
   $2\ell \mid 2\ell$ donc $n \mid m + \ell$.
   Donc i) est vraie.

3) On suppose $m = 2\ell$ et $n = 3\ell$.
   $\ell \mid 5\ell$ donc $\ell \mid m + n$.
   $2\ell \mid 2(2\ell)$ donc $m \mid n + \ell$.
   $3\ell \mid 3\ell$ donc $n \mid m + \ell$.
   Donc i) est vraie.

B] Montrons i) $\Longrightarrow$ ii).
On suppose i) vrai.
On distingue deux cas.

1) On suppose $\ell = 0$.
   $\ell \mid m + n$ et $\ell = 0$ donc $0 \mid m + n$ donc $m + n = 0$.
   $m \geqslant 0$, $n \geqslant 0$ et $m + n = 0$ donc $m = 0$ et $n = 0$.
   $m = \ell$ et $n = \ell$ donc ii) est vrai.

2) On suppose $\ell \neq 0$.
$\ell \in \mathbb{N}$ et $\ell \neq 0$ donc $\ell > 0$.
$m \geqslant \ell$ et $\ell > 0$ donc $m > 0$.
$n \geqslant m$ et $m > 0$ donc $n > 0$.
$m, \ell \in \mathbb{N}$ donc $m + \ell \in \mathbb{N}$. $n \in \mathbb{N}$, $m + \ell \in \mathbb{N}$ et $n \mid m + \ell$ donc il existe $a \in \mathbb{N}$ tel que $m + \ell = an$.
$m > 0$ et $\ell > 0$ donc $m + \ell > 0$ donc $an > 0$ donc $an \neq 0$ donc $a \neq 0$.
$m \leqslant n$ et $\ell \leqslant n$ donc $m + \ell \leqslant n + n$ donc $an \leqslant 2n$. $an \leqslant 2n$ et $n > 0$ donc $a \leqslant 2$.
$a \in \mathbb{N}$, $a \neq 0$ et $a \leqslant 2$ donc $a = 1$ ou $a = 2$.

a) On suppose $a = 1$.
$a = 1$ et $an = m + \ell$ donc $n = m + \ell$.
$n = m + \ell$ donc $n + \ell = m + 2\ell$. $m \mid n + \ell$ donc $m \mid m + 2\ell$.
$m \mid m + 2\ell$ et $m \mid m$ donc $m \mid (m + 2\ell) - m$. D'où $m \mid 2\ell$.
$m \in \mathbb{N}$, $2\ell \in \mathbb{N}$ et $m \mid 2\ell$ donc il existe $b \in \mathbb{N}$ tel que $2\ell = bm$.
$\ell > 0$ donc $2\ell > 0$ donc $bm > 0$ donc $bm \neq 0$ donc $b \neq 0$.
$\ell \leqslant m$ donc $2\ell \leqslant 2m$ donc $bm \leqslant 2m$. $bm \leqslant 2m$ et $m > 0$ donc $b \leqslant 2$.
$b \in \mathbb{N}$, $b \neq 0$ et $b \leqslant 2$ donc $b = 1$ ou $b = 2$.

- On suppose $b = 1$.
$b = 1$ et $bm = 2\ell$ donc $m = 2\ell$.
$n = m + \ell$ et $m = 2\ell$ donc $n = 3\ell$.
$m = 2\ell$ et $n = 3\ell$ donc ii) est vraie.

- On suppose $b = 2$.
$b = 2$ et $bm = 2\ell$ donc $2m = 2\ell$ donc $m = \ell$.
$n = m + \ell$ et $m = \ell$ donc $n = 2\ell$.
$m = \ell$ et $n = 2\ell$ donc ii) est vraie.

b) On suppose $a = 2$.
$a = 2$ et $an = m + \ell$ donc $2n = m + \ell$.
$m \leqslant n$, $\ell \leqslant n$ et $m + \ell = n + n$ donc $m = n$ et $\ell = n$.
$m = \ell$ et $n = \ell$ donc ii) est vraie.