Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2020/2021.

Corrigé du contrôle terminal d'arithmétique et de cryptographie

Exercice 1.

1) • 1re solution.
$9 = 4 + 1 \times 5$ donc $9 \equiv 4$ [5]. D'où $3^2 \equiv 2^2$ [5].
$3^2 \equiv 2^2$ [5] donc $(3^2)^k \equiv (2^2)^k$ [5]. D'où $3^{2k} \equiv 2^{2k}$ [5].

• 2e solution.
∗ $3^{2k} = (3^2)^k$ donc $3^{2k} = 9^k$.
$9 = -1 + 2 \times 5$ donc $9 \equiv -1$ [5] donc $9^k \equiv (-1)^k$ [5].
De ce qui précède, on déduit que $3^{2k} \equiv (-1)^k$ [5].

∗ $2^{2k} = (2^2)^k$ donc $2^{2k} = 4^k$.
$4 = -1 + 1 \times 5$ donc $4 \equiv -1$ [5] donc $4^k \equiv (-1)^k$ [5].
De ce qui précède, on déduit que $2^{2k} \equiv (-1)^k$ [5].

∗ $2^{2k} \equiv (-1)^k$ [5] donc $(-1)^k \equiv 2^{2k}$ [5].
$3^{2k} \equiv (-1)^k$ [5] et $(-1)^k \equiv 2^{2k}$ [5] donc $3^{2k} \equiv 2^{2k}$ [5].

2) ∗ $3^{6m} = 3^{3\times 2m} = (3^3)^{2m}$ donc $3^{6m} = 27^{2m}$.
$27 = -1 + 4 \times 7$ donc $27 \equiv -1$ [7] donc $27^2 \equiv (-1)^2$ [7]. D'où $27^2 \equiv 1$ [7].
$27^2 \equiv 1$ [7] donc $(27^2)^m \equiv 1^m$ [7]. D'où $27^{2m} \equiv 1$ [7].
De ce qui précède, on déduit que $3^{6m} \equiv 1$ [7].

∗ $2^{6m} = 2^{3\times 2m} = (2^3)^{2m}$ donc $2^{6m} = 8^{2m}$.
$8 = 1 + 1 \times 7$ donc $8 \equiv 1$ [7] donc $8^{2m} \equiv 1^{2m}$ [7]. D'où $8^{2m} \equiv 1$ [7].
De ce qui précède, on déduit que $2^{6m} \equiv 1$ [7].

∗ $2^{6m} \equiv 1$ [7] donc $1 \equiv 2^{6m}$ [7].
$3^{6m} \equiv 1$ [7] et $1 \equiv 2^{6m}$ [7] donc $3^{6m} \equiv 2^{6m}$ [7].

3) • 1re solution.
Grâce à 1) on a $3^{2\times 3n} \equiv 2^{2\times 3n}$ [5]. D'où $3^{6n} \equiv 2^{6n}$ [5]. $3^{6n} \equiv 2^{6n}$ [5] donc $5 \mid 3^{6n} - 2^{6n}$.
Par 2) on a $3^{6n} \equiv 2^{6n}$ [7]. D'où $7 \mid 3^{6n} - 2^{6n}$.
$3 \times 5 + (-2) \times 7 = 1$ donc 5 et 7 sont premiers entre eux.
$5 \mid 3^{6n} - 2^{6n}$, $7 \mid 3^{6n} - 2^{6n}$, 5 et 7 sont premiers entre eux donc $5 \times 7 \mid 3^{6n} - 2^{6n}$.
D'où $35 \mid 3^{6n} - 2^{6n}$.

• 2e solution.
On a vu que $3^{6n} = 27^{2n}$ et que $2^{6n} = 8^{2n}$.
$27 = -8 + 1 \times 35$ donc $27 \equiv -8$ [35]. $27 \equiv -8$ [35] donc $(27)^{2n} \equiv (-8)^{2n}$ [35].
$(-8)^{2n} = ((-1)8)^{2n} = (-1)^{2n} \times 8^{2n}$. $2n$ est pair donc $(-1)^{2n} = 1$. D'où $(-8)^{2n} = 8^{2n}$.
De ce qui précède, on déduit que $3^{6n} \equiv 2^{6n}$ [35].
$3^{6n} \equiv 2^{6n}$ [35] donc $35 \mid 3^{6n} - 2^{6n}$.

Exercice 2.

* $b \mid bd$ et $bd \mid ad + bc$ donc $b \mid ad + bc$.
  $b \mid ad + bc$ et $b \mid bc$ donc $b \mid (ad + bc) - bc$. D'où $b \mid ad$.
  $b \mid ad$ et b est premier avec a donc $b \mid d$.

* $d \mid bd$ et $bd \mid ad + bc$ donc $d \mid ad + bc$.
  $d \mid ad + bc$ et $d \mid ad$ donc $d \mid (ad + bc) - ad$. D'où $d \mid bc$.
  $d \mid cb$ et d est premier avec c donc $d \mid b$.

* $b \mid d$ et $d \mid b$ donc $b = d$ ou $b = -d$.

Exercice 3.

1) On distingue deux cas.

   * On suppose n pair.
     n est pair donc $n(n + 1)$ est pair.

   * On suppose n impair.
     n est impair donc $n + 1$ est pair donc $n(n + 1)$ est pair.

2) On a $2S_n = n(n + 1)$.
   On distingue deux cas.

   * On suppose n impair.
     n est impair donc $n + 1$ est pair donc $2 \mid n + 1$.
     $2 \mid n + 1$ et $2 \neq 0$ donc on dispose du quotient de $n + 1$ par 2, on le note q. Ainsi $n + 1 = 2q$.
     $2S_n = n(n + 1)$ donc $2S_n = 2(qn)$. $2 \neq 0$ donc $S_n = qn$.
     $S_n = qn$ donc n divise S_n. De plus, comme $n \neq 0$, le quotient de S_n par n vaut q.
     On en déduit que, dans la division euclidienne de S_n par n, le quotient vaut q et reste vaut 0.

   * On suppose n pair.
     n est pair donc $2 \mid n$.
     $2 \mid n$ et $2 \neq 0$ donc on dispose du quotient de n par 2, on le note q. Ainsi $n = 2q$.
     $2 \mid n$, $2 \neq 0$, $2 \in \mathbb{N}$ et $n \in \mathbb{N}$ donc le quotient de n par 2 est un entier naturel. Ainsi $q \in \mathbb{N}$.
     $n \neq 0$ donc $2q \neq 0$ donc $q \neq 0$. $q \in \mathbb{N}$ et $q \neq 0$ donc $q > 0$. $q > 0$ donc $q < 2q$. Ainsi $q < n$.
     $2S_n = n(n + 1)$ donc $2S_n = 2(q(n + 1))$. $2 \neq 0$ donc $S_n = q(n + 1)$.
     $S_n = qn + q$, $q \in \mathbb{N}$ et $q < |n|$ donc, dans la division euclidienne de S_n par n, le quotient vaut q et le reste vaut q.

Exercice 4.

- On constate que $(1,1) \in S$ et que $(3,3) \in S$. Donc $\{(1,1),(3,3)\} \subset S$.

- Soit $n \in \mathbb{N}^*$. On suppose $n \geqslant 5$. Montrons que $\sum_{k=1}^{n} k! \equiv 3\ [5]$.

  $n \geqslant 5$ donc $\sum_{k=1}^{n} k! = \sum_{k=1}^{4} k! + \sum_{k=5}^{n} k!$.

  $\forall k \geqslant 5\ 5 \mid k!$ donc $\forall k \in \{5,\dots,n\}\ 5 \mid k!$ donc $5 \mid \sum_{k=5}^{n} k!$. D'où $\sum_{k=5}^{n} k! \equiv 0\ [5]$.

  $\sum_{k=1}^{4} k! = 1+2+6+24 = 33$ donc $\sum_{k=1}^{4} k! = 3 + 6 \times 5$. D'où $\sum_{k=1}^{4} k! \equiv 3\ [5]$.

  $\sum_{k=1}^{4} k! \equiv 3\ [5]$ et $\sum_{k=5}^{n} k! \equiv 0\ [5]$ donc $\sum_{k=1}^{4} k! + \sum_{k=5}^{n} k! \equiv 3+0\ [5]$. D'où $\sum_{k=1}^{n} k! \equiv 3\ [5]$.

- Soit $a \in \mathbb{Z}$. Justifions que $a^2 \equiv 0\ [5]$ ou $a^2 \equiv 1\ [5]$ ou $a^2 \equiv 4\ [5]$.
  $a \equiv 0\ [5]$ ou $a \equiv 1\ [5]$ ou $a \equiv 2\ [5]$ ou $a \equiv 3\ [5]$ ou $a \equiv 4\ [5]$ donc
  $a^2 \equiv 0^2\ [5]$ ou $a^2 \equiv 1^2\ [5]$ ou $a^2 \equiv 2^2\ [5]$ ou $a^2 \equiv 3^2\ [5]$ ou $a^2 \equiv 4^2\ [5]$ donc
  $a^2 \equiv 0\ [5]$ ou $a^2 \equiv 1\ [5]$ ou $a^2 \equiv 4\ [5]$ ou $a^2 \equiv 9\ [5]$ ou $a^2 \equiv 16\ [5]$.
  $9 \equiv 4\ [5]$ et $16 \equiv 1\ [5]$ donc $a^2 \equiv 0\ [5]$ ou $a^2 \equiv 1\ [5]$ ou $a^2 \equiv 4\ [5]$ ou $a^2 \equiv 4\ [5]$ ou $a^2 \equiv 1\ [5]$
  donc $a^2 \equiv 0\ [5]$ ou $a^2 \equiv 1\ [5]$ ou $a^2 \equiv 4\ [5]$.

- Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On suppose $\sum_{k=1}^{n} k! = a^2$. Justifions que $n \leqslant 4$.

  On suppose, par l'absurde, que $n \geqslant 5$.

  $n \geqslant 5$ donc $\sum_{k=1}^{n} k! \equiv 3\ [5]$. $a^2 \equiv 3\ [5]$ donc $3 \equiv a^2\ [5]$.

  $3 \equiv a^2\ [5]$ et $(a^2 \equiv 0\ [5]$ ou $a^2 \equiv 1\ [5]$ ou $a^2 \equiv 4\ [5])$ donc $3 \equiv 0\ [5]$ ou $3 \equiv 1\ [5]$ ou $3 \equiv 4\ [5]$.
  $(3 \equiv 0\ [5]$ ou $3 \equiv 1\ [5]$ ou $3 \equiv 4\ [5])$ et $0 \leqslant 3, 0, 1, 4 < 5$ donc $3 = 0$ ou $3 = 1$ ou $3 = 4$. Absurde.

- Montrons que $S \subset \{(1,1),(3,3)\}$.
  Soit $(n,a) \in S$.

  Alors $n \in \mathbb{N}^*$, $a \in \mathbb{N}$ et $\sum_{k=1}^{n} k! = a^2$.

  Grâce à ce qui précède, on a $n \leqslant 4$.

  Justifions que $n \neq 2$. Supposons, par l'absurde, que $n = 2$. $\sum_{k=1}^{2} k! = 3$ donc $a^2 = 3$. Contradiction.

  Justifions que $n \neq 4$. Supposons, par l'absurde, que $n = 4$. $\sum_{k=1}^{4} k! = 33$ donc $a^2 = 33$. Contradiction.

  On en déduit que $n = 1$ ou $n = 3$.
  Si $n = 1$, alors $1 = a^2$ donc (car $a \geqslant 0$) $a = 1$, puis $(n,a) = (1,1)$.
  Si $n = 3$, alors $9 = a^2$ donc (car $a \geqslant 0$) $a = 3$, puis $(n,a) = (3,3)$.
  $(n,a) = (1,1)$ ou $(n,a) = (3,3)$ donc $(n,a) \in \{(1,1),(3,3)\}$.

- Concluons.
  $\{(1,1),(3,3)\} \subset S$ et $S \subset \{(1,1),(3,3)\}$ donc $S = \{(1,1),(3,3)\}$.