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

Corrigé du contrôle continu d'arithmétique et de cryptographie

Exercice 1.

On procède par récurrence.

* $4^0 + 6 \times 0 - 1 = 1 + 0 - 1 = 0$. $9 \mid 0$ donc $9 \mid 4^0 + 6 \times 0 - 1$.

* Soit $n \in \mathbb{N}$. On suppose que $9 \mid 4^n + 6n - 1$.

$$\begin{aligned} 4^{n+1} + 6(n+1) - 1 &= 4^n \times 4^1 + 6(n+1) - 1 \\ &= 4 \times 4^n + 6(n+1) - 1 \\ &= 4\Big(4^n + (6n-1) - (6n-1)\Big) + 6(n+1) - 1 \\ &= 4\Big(4^n + (6n-1)\Big) - 4(6n-1) + 6(n+1) - 1 \\ &= 4\Big(4^n + (6n-1)\Big) - 18n + 9 \\ &= 4\Big(4^n + (6n-1)\Big) + (1-2n)9 \end{aligned}$$

$9 \mid 4^n + 6n - 1$ et $9 \mid 9$ donc $9 \mid 4\Big(4^n + (6n-1)\Big) + (1-2n)9$. D'où $9 \mid 4^{n+1} + 6(n+1) - 1$.

Exercice 2.

* $2^{6k+1} = 2^{6k} \times 2^1 = 2 \times (2^6)^k$. De plus $2^6 = 2^{3\times 2} = (2^3)^2 = 8^2 = 64$. Donc $2^{6k+1} = 2 \times 64^k$.
  $64 = 66 - 2$ donc $64 = -2 + 6 \times 11$ donc $64 \equiv -2$ [11].
  $64 \equiv -2$ [11] et $k \in \mathbb{N}$ donc $64^k \equiv (-2)^k$ [11] donc $2 \times 64^k \equiv 2(-2)^k$ [11].
  De ce qui précède, on déduit que $2^{6k+1} \equiv 2(-2)^k$ [11].

* $3^{2k+2} = 3^{2k} \times 3^2 = (3^2)^k \times 9$. Donc $3^{2k+2} = 9 \times 9^k$.
  $9 = 11 - 2$ donc $9 = -2 + 1 \times 11$ donc $9 \equiv -2$ [11].
  $9 \equiv -2$ [11] et $k \in \mathbb{N}$ donc $9^k \equiv (-2)^k$ [11] donc $9 \times 9^k \equiv 9(-2)^k$ [11].
  De ce qui précède, on déduit que $3^{2k+2} \equiv 9(-2)^k$ [11].

* $2^{6k+1} \equiv 2(-2)^k$ [11] et $3^{2k+2} \equiv 9(-2)^k$ [11] donc $2^{6k+1} + 3^{2k+2} \equiv 2(-2)^k + 9(-2)^k$ [11].
  $2(-2)^k + 9(-2)^k = (2+9)(-2)^k = 11(-2)^k$. $(-2)^k \times 11 \equiv 0$ [11] donc $2(-2)^k + 9(-2)^k \equiv 0$ [11].
  $2^{6k+1} + 3^{2k+2} \equiv 2(-2)^k + 9(-2)^k$ [11] et $2(-2)^k + 9(-2)^k \equiv 0$ [11] donc $2^{6k+1} + 3^{2k+2} \equiv 0$ [11].

Exercice 3.

On suppose, par l'absurde, que $A \neq \varnothing$.
$A \neq \varnothing$ donc il existe $x \in A$. $x \in A$ donc $3x \mid x^2 + 1$.
$x \mid 3x$ et $3x \mid x^2 + 1$ donc $x \mid x^2 + 1$. $x \mid x^2 + 1$ et $x \mid xx$ donc $x \mid (x^2 + 1) - xx$. Donc $x \mid 1$.
$x \mid 1$ donc ($x = 1$ ou $x = -1$). ($x = 1$ ou $x = -1$) donc $x^2 = 1$.
$3 \mid 3x$ et $3x \mid x^2 + 1$ donc $3 \mid x^2 + 1$.
$x^2 = 1$ donc $x^2 + 1 = 2$. $3 \mid x^2 + 1$ donc $3 \mid 2$.
$3 \mid 2$ donc $3 \in \mathrm{Div}(2)$ donc $3 \in \{-2, -1, 1, 2\}$. Contradiction.

Exercice 4.

$\{1,2\}+\{2,3,4\}=\{1+2,1+3,1+4,2+2,2+3,2+4\}=\{3,4,5,4,5,6\}=\{3,4,5,6\}$.
$3,4,5$ et 6 sont deux à deux distincts donc $\{3,4,5,6\}$ a quatre éléments.
Donc $\{1,2\}+\{2,3,4\}$ a quatre éléments.

Exercice 5.

1) $a \mid b$ et $a \in \mathbb{N}$ donc $a^a \mid b^a$.
   $a, b \in \mathbb{N}$, $a \mid b$ et $b \neq 0$ donc $a \leqslant b$. $a, b \in \mathbb{N}$ et $a \leqslant b$ donc $b^a \mid b^b$.
   $a^a \mid b^a$ et $b^a \mid b^b$ donc $a^a \mid b^b$.

2) On va montrer que 4 et 10 conviennent.

   * On remarque que $4 \in \mathbb{N}^*$ et $10 \in \mathbb{N}^*$.

   * Justifions que $4 \nmid 10$.
     Supposons, par l'absurde, que $4 \mid 10$.
     $4 \mid 10$ donc $2 \times 2 \mid 2 \times 5$. $2 \times 2 \mid 2 \times 5$ et $2 \neq 0$ donc $2 \mid 5$.
     $2 \mid 5$ donc $2 \in \mathrm{Div}(5)$ donc $2 \in \{-5,-1,1,5\}$. Contradiction.

   * Vérifions que $4^4 \mid 10^{10}$.
     $4^4 = (2^2)^4 = 2^{2\times 4} = 2^8$ donc $4^4 = 2^8$.
     $10^{10} = (2\times 5)^{10} = 2^{10} \times 5^{10}$ donc $10^{10} = 5^{10} \times 2^{10}$.
     $8, 10 \in \mathbb{N}$ et $8 \leqslant 10$ donc $2^8 \mid 2^{10}$.
     $2^8 \mid 2^{10}$ donc $2^8 \mid 5^{10} \times 2^{10}$ donc $4^4 \mid 10^{10}$.

Exercice 6.

1) On distingue deux cas.
   * On suppose $n = 0$.
     $n = 0$ donc $a^n - b^n = a^0 - b^0 = 1 - 1 = 0$. $a - b \mid 0$ donc $a - b \mid a^n - b^n$.
   * On suppose $n \neq 0$.
     $n \in \mathbb{N}^*$ donc $a^n - b^n = (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right)$.
     $(a-b) \mid (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right)$ donc $a - b \mid a^n - b^n$.

2) Par 1) on a, $a-(-c) \mid a^n - (-c)^n$.
   $(-c)^n = ((-1)c)^n = (-1)^n c^n$. n est impair donc $(-1)^n = -1$. D'où $(-c)^n = -c^n$.
   $a-(-c) \mid a^n - (-c)^n$ donne $a + c \mid a^n + c^n$.

3) a) On suppose que $a \in \{-3,-2,0,1\}$.

      On traite les cas un par un.

∗ On suppose $a = -3$.
$a = -3$ donc $a + 1 = -2$.
$-3 = 1 - 4$ donc $-3 = 1 + (-2) \times 2$ donc $-3 \equiv 1$ [2].
$-3 \equiv 1$ [2] et $n \in \mathbb{N}$ donc $(-3)^n \equiv 1^n$ [2]. $(-3)^n \equiv 1$ [2] donc $(-3)^n + 1 \equiv 1 + 1$ [2].
$(-3)^n + 1 \equiv 2$ [2] et $2 \equiv 0$ [2] donc $(-3)^n + 1 \equiv 0$ [2] donc $2 \mid (-3)^n + 1$.
$2 \mid (-3)^n + 1$ donc $-2 \mid (-3)^n + 1$ donc $a + 1 \mid a^n + 1$.

∗ On suppose $a = -2$.
$a = -2$ donc $a + 1 = -1$. $-1 \mid a^n + 1$ donc $a + 1 \mid a^n + 1$.

∗ On suppose $a = 0$.
$a = 0$ donc $a + 1 = 1$. $1 \mid a^n + 1$ donc $a + 1 \mid a^n + 1$.

∗ On suppose $a = 1$.
$a = 1$ donc $a + 1 = 2$.
$a = 1$ donc $a^n + 1 = 1^n + 1 = 1 + 1 = 2$.
$2 \mid 2$ donc $a + 1 \mid a^n + 1$.

b) $a = (a + 1) - 1$ donc $a = -1 + 1 \times (a + 1)$ donc $a \equiv -1$ $[a + 1]$.
$a \equiv -1$ $[a + 1]$ et $n \in \mathbb{N}$ donc $a^n \equiv (-1)^n$ $[a + 1]$.

c) On va prouver les deux implications.

∗ Justifions que ii) $\Longrightarrow$ i).
On suppose ii).
n est impair ou $a \in \{-3, -2, 0, 1\}$.
Si n est impair, alors (par 2)) $a + 1$ divise $a^n + 1^n$ donc $a + 1$ divise $a^n + 1$.
Si $a \in \{-3, -2, 0, 1\}$, alors (par a)) $a + 1$ divise $a^n + 1$.
Donc i) est vrai.

∗ Montrons que i) $\Longrightarrow$ ii).
On suppose i).
i) se traduit par $a + 1 \mid a^n + 1$.
On distingue deux cas.
⋆ On suppose n impair.
n est impair donc ii) est vrai.
⋆ On suppose n pair.
- Montrons que $a + 1 \mid a^n - 1$.
b) donne $a^n \equiv (-1)^n$ $[a+1]$. n est pair donc $(-1)^n = 1$. $a^n \equiv 1$ $[a+1]$ donc $a+1 \mid a^n - 1$.
On peut aussi dire que (par 1)) $a - (-1) \mid a^n - (-1)^n$. D'où $a + 1 \mid a^n - 1$.
- Concluons.
$a + 1 \mid a^n + 1$ et $a + 1 \mid a^n - 1$ donc $a + 1 \mid (a^n + 1) - (a^n - 1)$. D'où $a + 1 \mid 2$.
$a + 1 \mid 2$ donc $a + 1 \in \text{Div}(2)$ donc $a + 1 \in \{-2, -1, 1, 2\}$.
$a + 1$ vaut $-2, -1, 1$ ou 2 donc a vaut $-3, -2, 0$ ou 1. D'où $a \in \{-3, -2, 0, 1\}$.