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

Corrigé du contrôle continu d'arithmétique et de cryptographie

Exercice 1.

- $2^{6n+3} = 2^{6n} \times 2^3 = (2^6)^n \times 8$ donc $2^{6n+3} = 64^n \times 8$.
  $64 = 68 - 4 = 4 \times 17 - 4$ donc $64 = (-4) + 4 \times 17$. D'où $64 \equiv -4$ [17].
  $64 \equiv -4$ [17] et $n \in \mathbb{N}$ donc $64^n \equiv (-4)^n$ [17] donc $64^n \times 8 \equiv (-4)^n \times 8$ [17].
  De ce qui précède, on déduit que $2^{6n+3} \equiv (-4)^n \times 8$ [17].

- $3^{4n+2} = 3^{4n} \times 3^2 = (3^4)^n \times 9$ donc $3^{4n+2} = 81^n \times 9$.
  $81 = 85 - 4 = 5 \times 17 - 4$ donc $81 = (-4) + 5 \times 17$. D'où $81 \equiv -4$ [17].
  $81 \equiv -4$ [17] et $n \in \mathbb{N}$ donc $81^n \equiv (-4)^n$ [17] donc $81^n \times 9 \equiv (-4)^n \times 9$ [17].
  De ce qui précède, on déduit que $3^{4n+2} \equiv (-4)^n \times 9$ [17].

- $2^{6n+3} \equiv (-4)^n \times 8$ [17] et $3^{4n+2} \equiv (-4)^n \times 9$ [17] donc $2^{6n+3} + 3^{4n+2} \equiv (-4)^n \times 8 + (-4)^n \times 9$ [17].
  $(-4)^n \times 8 + (-4)^n \times 9 = (-4)^n \times (8+9)$ donc $(-4)^n \times 8 + (-4)^n \times 9 = (-4)^n \times 17$.
  $(-4)^n \times 17 \equiv 0$ [17] donc $(-4)^n \times 8 + (-4)^n \times 9 \equiv 0$ [17].
  $2^{6n+3} + 3^{4n+2} \equiv (-4)^n \times 8 + (-4)^n \times 9$ [17] et $(-4)^n \times 8 + (-4)^n \times 9 \equiv 0$ [17] donc $2^{6n+3} + 3^{4n+2} \equiv 0$ [17].

- $2^{6n+3} + 3^{4n+2} \equiv 0$ [17] donc $17 \mid 2^{6n+3} + 3^{4n+2}$.

Exercice 2.

Notons r le reste dans la division euclidienne de $b-1$ par a. Ainsi $b - 1 = qa + r$ et $0 \leqslant r < |a|$.
$a \in \mathbb{N}^*$ donc $a \in \mathbb{Z}$ et $a > 0$. $a \geqslant 0$ donc $|a| = a$. D'où $r < a$.

- $b-1 = qa+r$ donc $(b-1)a^n = (qa+r)a^n$ donc $ba^n - 1a^n = (qa)a^n + ra^n$ donc $ba^n - a^n = qa^{n+1} + ra^n$ donc $ba^n = (qa^{n+1} + ra^n) + a^n$ donc $ba^n = qa^{n+1} + (r+1)a^n$ donc $ba^n - 1 = qa^{n+1} + ((r+1)a^n - 1)$.

- $r \geqslant 0$ donc $r + 1 > 0$. $a > 0$ donc $a^n > 0$. $r + 1 > 0$ et $a^n > 0$ donc $(r+1)a^n > 0$.
  $(r+1)a^n \in \mathbb{Z}$ et $(r+1)a^n > 0$ donc $(r+1)a^n \geqslant 1$ donc $(r+1)a^n - 1 \geqslant 0$.

- $r, a \in \mathbb{Z}$ et $r < a$ donc $r + 1 \leqslant a$.
  $a \geqslant 0$ donc $a^n \geqslant 0$.
  $r + 1 \leqslant a$ et $a^n \geqslant 0$ donc $a^n(r+1) \leqslant a^n a$ donc $(r+1)a^n \leqslant a^{n+1}$ donc $(r+1)a^n - 1 < a^{n+1}$.
  $a \geqslant 0$ donc $a^{n+1} \geqslant 0$ donc $|a^{n+1}| = a^{n+1}$. D'où $(r+1)a^n - 1 < |a^{n+1}|$.

- $ba^n - 1 = qa^{n+1} + ((r+1)a^n - 1)$ et $0 \leqslant (r+1)a^n - 1 < |a^{n+1}|$ donc, dans la division euclidienne de $ba^n - 1$ par a^{n+1}, le quotient vaut q (et le reste vaut $(r+1)a^n - 1$).

Exercice 3.

On va procéder par récurrence. Pour tout $n \in \mathbb{N}^*$, on note $\mathcal{P}(n)$ l'assertion suivante : $21 \mid 2^{4^n} + 5$.

- $2^{4^1} + 5 = 2^4 + 5 = 16 + 5 = 21$.
  $21 \mid 21$ donc $21 \mid 2^{4^1} + 5$ donc $\mathcal{P}(1)$ est vraie.

- Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}(n)$.
  $21 \mid 2^{4^n} + 5$ donc $2^{4^n} + 5 \equiv 0\ [21]$ donc $\left(2^{4^n} + 5\right) - 5 \equiv 0 - 5\ [21]$ donc $2^{4^n} \equiv -5\ [21]$.
  $2^{4^n} \equiv -5\ [21]$ et $4 \in \mathbb{N}$ donc $\left(2^{4^n}\right)^4 \equiv (-5)^4\ [21]$.
  $\left(2^{4^n}\right)^4 = 2^{4^n \times 4} = 2^{4^n \times 4^1} = 2^{4^{n+1}}$. 4 est pair donc $(-5)^4 = 5^4$. D'où $2^{4^{n+1}} \equiv 5^4\ [21]$.
  $5^4 = 5^{2\times 2} = \left(5^2\right)^2$ donc $5^4 = 25^2$.
  $21 \mid 21$ donc $21 \mid 25 - 4$ donc $25 \equiv 4\ [21]$. $25 \equiv 4\ [21]$ et $2 \in \mathbb{N}$ donc $25^2 \equiv 4^2\ [21]$. D'où $5^4 \equiv 16\ [21]$.
  $2^{4^{n+1}} \equiv 5^4\ [21]$ et $5^4 \equiv 16\ [21]$ donc $2^{4^{n+1}} \equiv 16\ [21]$.
  $16 = 21 - 5$ donc $16 = (-5) + 1 \times 21$ donc $16 \equiv -5\ [21]$.
  $2^{4^{n+1}} \equiv 16\ [21]$ et $16 \equiv -5\ [21]$ donc $2^{4^{n+1}} \equiv -5\ [21]$.
  $2^{4^{n+1}} \equiv -5\ [21]$ donc $21 \mid 2^{4^{n+1}} - (-5)$ donc $21 \mid 2^{4^{n+1}} + 5$ donc $\mathcal{P}(n+1)$ est vraie.

Exercice 4.

$a \neq 0$ donc, pour tout $b \in \mathbb{Z}$, on peut appliquer le théorème de division euclidienne. Il peut s'énoncer ainsi : pour tout $b \in \mathbb{Z}$ il existe un et un seul $(q, r) \in \mathbb{Z} \times [\![0, |a| - 1]\!]$ tel que $b = qa + r$.
Autrement dit : pour tout $b \in \mathbb{Z}$, il existe un et un seul $(q, r) \in \mathbb{Z} \times [\![0, |a| - 1]\!]$ tel que $\varphi(q, r) = b$.
φ est donc bijective.

Exercice 5.

1) - Soit $(x, y) \in S$.
   $(x, y) \in S$ donc $x^2 - y^2 - 4x - 2y = -2$.

$$\begin{aligned} x^2 - y^2 - 4x - 2y &= (x^2 - 4x) - (y^2 + 2y) \\ &= (x^2 - 4x + 4 - 4) - (y^2 + 2y + 1 - 1) \\ &= (x^2 - 4x + 4) - (y^2 + 2y + 1) - 4 - (-1) \\ &= (x-2)^2 - (y+1)^2 - 3 \\ &= ((x-2) + (y+1))((x-2) - (y+1)) - 3 \\ &= (x + y - 1)(x - y - 3) - 3 \end{aligned}$$

   $x^2 - y^2 - 4x - 2y = -2$ donc $(x + y - 1)(x - y - 3) - 3 = -2$. D'où $(x + y - 1)(x - y - 3) = 1$.
   $1 = (x + y - 1)(x - y - 3)$ donc $x - y - 3 \mid 1$ donc $x - y - 3 = -1$ ou $x - y - 3 = 1$.

   * On suppose que $x - y - 3 = -1$.
     $x - y - 3 = -1$ et $1 = (x + y - 1)(x - y - 3)$ donc $x + y - 1 = -1$.
     $x + y - 1 = -1$ et $x - y - 3 = -1$ donc $(x + y - 1) + (x - y - 3) = (-1) + (-1)$ donc $2x - 4 = -2$ donc $x = 1$. $x - y - 3 = -1$ et $x = 1$ donc $1 - y - 3 = -1$ donc $y = -1$.
     $x = 1$ et $y = -1$ donc $(x, y) = (1, -1)$.

   * On suppose que $x - y - 3 = 1$.
     $x - y - 3 = 1$ et $1 = (x + y - 1)(x - y - 3)$ donc $x + y - 1 = 1$.
     $x + y - 1 = 1$ et $x - y - 3 = 1$ donc $(x + y - 1) + (x - y - 3) = 1 + 1$ donc $2x - 4 = 2$ donc $x = 3$. $x - y - 3 = 1$ et $x = 3$ donc $3 - y - 3 = 1$ donc $y = -1$.
     $x = 3$ et $y = -1$ donc $(x, y) = (3, -1)$.

   * On a montré que $(x, y) = (1, -1)$ ou $(x, y) = (3, -1)$. D'où $(x, y) \in \{(1, -1), (3, -1)\}$.

   - $\forall (x, y) \in S$ $(x, y) \in \{(1, -1), (3, -1)\}$ donc $S \subset \{(1, -1), (3, -1)\}$.

2) • $(1,-1) \in \mathbb{Z} \times \mathbb{Z}$ et $1^2 - (-1)^2 - 4 \times 1 - 2 \times (-1) = -2$ donc $(1,-1) \in S$.

• $(3,-1) \in \mathbb{Z} \times \mathbb{Z}$ et $3^2 - (-1)^2 - 4 \times 3 - 2 \times (-1) = -2$ donc $(3,-1) \in S$.

• $(1,-1) \in S$ et $(3,-1) \in S$ donc $\forall (x,y) \in \{(1,-1),(3,-1)\}$ $(x,y) \in S$ donc : $\{(1,-1),(3,-1)\} \subset S$.

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