Université de la Réunion. 1re année de licence de mathématiques. Année universitaire 2021/2022.

Corrigé du contrôle continu d'arithmétique et de cryptographie

Exercice 1.

- ∗ Soit $x \in A$.
  $2x^2 - 1 \mid x$ donc $2x^2 - 1 \mid (2x)x$. D'où $2x^2 - 1 \mid 2x^2$.
  $2x^2 - 1 \mid 2x^2$ et $2x^2 - 1 \mid 2x^2 - 1$ donc $2x^2 - 1 \mid 2x^2 - (2x^2 - 1)$. D'où $2x^2 - 1 \mid 1$.
  $2x^2 - 1 \mid 1$ donc $2x^2 - 1 = -1$ ou $2x^2 - 1 = 1$.
  On distingue donc deux cas.
  — On suppose $2x^2 - 1 = -1$.
  $2x^2 - 1 = -1$ donc $2x^2 = 0$ donc $x^2 = 0$ donc $x = 0$.
  — On suppose $2x^2 - 1 = 1$.
  $2x^2 - 1 = 1$ donc $2x^2 = 2$ donc $x^2 = 1$ donc $x = -1$ ou $x = 1$.
  On a donc $x = 0$ ou ($x = -1$ ou $x = 1$). On en déduit $x \in \{-1, 0, 1\}$.
  ∗ Ce qui précède montre que $\forall x \in A\ x \in \{-1, 0, 1\}$. On en déduit $A \subset \{-1, 0, 1\}$.

- Vérifions que $\{-1, 0, 1\} \subset A$.
  $2(-1)^2 - 1 = 1$. $\forall b \in \mathbb{Z}\ 1 \mid b$ donc $1 \mid -1$. $2(-1)^2 - 1 \mid -1$ donc $-1 \in A$.
  $2 \times 0^2 - 1 = -1$. $\forall a \in \mathbb{Z}\ a \mid 0$ donc $-1 \mid 0$. $2 \times 0^2 - 1 \mid 0$ donc $0 \in A$.
  $2 \times 1^2 - 1 = 1$. $\forall b \in \mathbb{Z}\ 1 \mid b$ donc $1 \mid 1$. $2 \times 1^2 - 1 \mid 1$ donc $1 \in A$.
  $-1 \in A$, $0 \in A$ et $1 \in A$ donc $\{-1, 0, 1\} \subset A$.

- Concluons.
  $A \subset \{-1, 0, 1\}$ et $\{-1, 0, 1\} \subset A$ donc $A = \{-1, 0, 1\}$.

Exercice 2.

- $8^0 - 7 \times 0 - 1 = 1 - 0 - 1 = 0$. $49 \mid 0$ donc $49 \mid 8^0 - 7 \times 0 - 1$ donc $P(0)$ est vraie.

- Soit $n \in \mathbb{N}$. On suppose $P(n)$ vraie.

$$\begin{aligned} 8^{n+1} - 7(n+1) - 1 &= 8^n \times 8^1 - (7n+7) - 1 \\ &= 8 \times 8^n - 7n - 8 \\ &= 8((8^n - 7n - 1) + (7n + 1)) - 7n - 8 \\ &= 8(8^n - 7n - 1) + 8(7n + 1) - 7n - 8 \\ &= 8(8^n - 7n - 1) + (56n + 8) - 7n - 8 \\ &= 8(8^n - 7n - 1) + 49n \end{aligned}$$

  $49 \mid 8^n - 7n - 1$ donc $49 \mid 8(8^n - 7n - 1)$.
  $49 \mid 8(8^n - 7n - 1)$ et $49 \mid 49n$ donc $49 \mid 8(8^n - 7n - 1) + 49n$. D'où $49 \mid 8^{n+1} - 7(n+1) - 1$.
  Donc $P(n+1)$ est vraie.

Exercice 3.

On distingue deux cas.

- On suppose $a = 1$.
  $b = b \times 1 + 0$ et $0 \leqslant 0 < |1|$ donc, dans la division euclidienne de b par 1, le quotient vaut b et le reste vaut 0.

- On suppose $a \neq 1$.
  $a \in \mathbb{N}$, $a \neq 0$ et $a \neq 1$ donc $a \geqslant 2$.
  On remarque que $b = (\alpha - 1)a + (a - 2)$.
  $a \geqslant 2$ donc $a - 2 \geqslant 0$. $2 > 0$ donc $a - 2 < a$. $a \in \mathbb{N}$ donc $a \geqslant 0$ donc $|a| = a$. D'où $a - 2 < |a|$.
  $b = (\alpha - 1)a + (a - 2)$ et $0 \leqslant a - 2 < |a|$ donc, dans la division euclidienne de b par a,
  le quotient vaut $\alpha - 1$ et le reste vaut $a - 2$.

Exercice 4.

Par définition, $b = qa + r$ et $0 \leqslant r < |a|$. Par définition, $b' = q'a + r'$ et $0 \leqslant r' < |a|$.
$(qa+r)(q'a+r') = (qa)(q'a)+(qa)r'+r(q'a)+rr' = (qaq')a+(qr')a+(rq')a+rr' = (qaq'+qr'+rq')a+rr'$
donc $bb' = (qaq' + qr' + rq')a + rr'$.
$r \geqslant 0$ et $r' \geqslant 0$ donc $rr' \geqslant 0$. Par hypothèse on a $rr' < |a|$. D'où $0 \leqslant rr' < |a|$.
$bb' = (qaq' + qr' + rq')a + rr'$ et $0 \leqslant rr' < |a|$ donc $qaq' + qr' + rq'$ est le quotient et rr' est le reste dans la division euclidienne de bb' par a.

Exercice 5.

1) • Soient $a, b \in \mathbb{Z}$.
  Montrons que les assertions suivantes sont équivalentes :
  i) $ab = 3$;
  ii) ($a = -3$ et $b = -1$) ou ($a = -1$ et $b = -3$) ou ($a = 1$ et $b = 3$) ou ($a = 3$ et $b = 1$).
  ∗ Vérifions ii) $\Longrightarrow$ i).
  C'est immédiat.
  ∗ Montrons i) $\Longrightarrow$ ii).
  On suppose i) vrai.
  $ab = 3$ donc $3 = ba$ donc $a \mid 3$ donc $a \in \mathrm{Div}(3)$.
  $\mathrm{Div}(3) = \{-3, -1, 1, 3\}$ donc $a \in \{-3, -1, 1, 3\}$ donc $a = -3$ ou $a = -1$ ou $a = 1$ ou $a = 3$.
  On distingue donc quatre cas.
  — On suppose $a = -3$.
  $ab = 3$ donc $(-3)b = (-3)(-1)$. $-3 \neq 0$ donc $b = -1$.
  — On suppose $a = -1$.
  $ab = 3$ donc $(-1)b = 3$ donc $b = -3$.
  — On suppose $a = 1$.
  $ab = 3$ donc $1b = 3$ donc $b = 3$.
  — On suppose $a = 3$.
  $ab = 3$ donc $3b = 3 \times 1$. $3 \neq 0$ donc $b = 1$.

- ∗ Soit $(x, y) \in A$.
  $(x - y)(2x - y) = 3$ donc : ($x - y = -3$ et $2x - y = -1$) ou ($x - y = -1$ et $2x - y = -3$) ou ($x - y = 1$ et $2x - y = 3$) ou ($x - y = 3$ et $2x - y = 1$).

On distingue donc quatre cas.
— On suppose $x-y=-3$ et $2x-y=-1$.
$(2x-y)-(x-y)=(-1)-(-3)$ donc $x=2$.
$x-y=-3$ donc $2-y=-3$ donc $y=5$. D'où $(x,y)=(2,5)$.
— On suppose $x-y=-1$ et $2x-y=-3$.
$(2x-y)-(x-y)=(-3)-(-1)$ donc $x=-2$.
$x-y=-1$ donc $(-2)-y=-1$ donc $y=-1$. D'où $(x,y)=(-2,-1)$.
— On suppose $x-y=1$ et $2x-y=3$.
$(2x-y)-(x-y)=3-1$ donc $x=2$.
$x-y=1$ donc $2-y=1$ donc $y=1$. D'où $(x,y)=(2,1)$.
— On suppose $x-y=3$ et $2x-y=1$.
$(2x-y)-(x-y)=1-3$ donc $x=-2$.
$x-y=3$ donc $(-2)-y=3$ donc $y=-5$. D'où $(x,y)=(-2,-5)$.
$(x,y)=(2,5)$ ou $(x,y)=(-2,-1)$ ou $(x,y)=(2,1)$ ou $(x,y)=(-2,-5)$ donc $(x,y)\in\{(2,5),(-2,-1),(2,1),(-2,-5)\}$.

∗ Ce qui précède montre que $\forall (x,y)\in A\ (x,y)\in\{(2,5),(-2,-1),(2,1),(-2,-5)\}$.
On en déduit que $A\subset\{(2,5),(-2,-1),(2,1),(-2,-5)\}$.

∗ On constate que $(2,5)\in A$, $(-2,-1)\in A$, $(2,1)\in A$ et $(-2,-5)\in A$.
On en déduit que $\{(2,5),(-2,-1),(2,1),(-2,-5)\}\subset A$.

∗ Conclusion.
$A\subset\{(2,5),(-2,-1),(2,1),(-2,-5)\}$ et $\{(2,5),(-2,-1),(2,1),(-2,-5)\}\subset A$ donc $A=\{(2,5),(-2,-1),(2,1),(-2,-5)\}$.

2) • $\forall x,y\in\mathbb{Z}\ xy-(x+y-2)=(xy-x)-y+2=x(y-1)-(y-1)+1=(x-1)(y-1)+1$.
Donc $B=\{(x,y)\in\mathbb{Z}\times\mathbb{Z}\mid (x-1)(y-1)=-1\}$.

• Soient $a,b\in\mathbb{Z}$.
Vérifions que les assertions suivantes sont équivalentes :
i) $ab=-1$;
ii) ($a=-1$ et $b=1$) ou ($a=1$ et $b=-1$).

∗ Vérifions ii) $\Longrightarrow$ i).
C'est immédiat.

∗ Vérifions i) $\Longrightarrow$ ii).
On suppose i) vrai.
$a\mid ab$ donc $a\mid -1$ donc $a=-1$ ou $a=1$.
On distingue donc deux cas.
— On suppose $a=-1$.
$ab=-1$ donc $(-1)b=-1$ donc $b=1$.
— On suppose $a=1$.
$ab=1$ donc $1b=-1$ donc $b=-1$.

• ∗ Soit $(x,y)\in\mathbb{Z}\times\mathbb{Z}$.
On a les équivalences successives suivantes :

$$\begin{aligned}(x,y)\in A &\iff (x-1)(y-1)=-1\\ &\iff (x-1=-1 \text{ et } y-1=1) \text{ ou } (x-1=1 \text{ et } y-1=-1)\\ &\iff (x=0 \text{ et } y=2) \text{ ou } (x=2 \text{ et } y=0)\\ &\iff (x,y)=(0,2) \text{ ou } (x,y)=(2,0)\\ &\iff (x,y)\in\{(0,2),(2,0)\}\end{aligned}$$

∗ $A\subset\mathbb{Z}\times\mathbb{Z}$, $\{(0,2),(2,0)\}\subset\mathbb{Z}\times\mathbb{Z}$ et $\forall (x,y)\in\mathbb{Z}\times\mathbb{Z}\ \Big((x,y)\in A\iff (x,y)\in\{(0,2),(2,0)\}\Big)$ donc $A=\{(0,2),(2,0)\}$.

Exercice 6.

A] $\alpha+\beta \mid \gamma$ et $\gamma \neq 0$ donc $|\alpha+\beta| \leqslant |\gamma|$.
$|\alpha|-|\beta| \leqslant |\alpha+\beta|$ ($|(\alpha+\beta)+(-\beta)| \leqslant |\alpha+\beta|+|-\beta|$ donc $|\alpha| \leqslant |\alpha+\beta|+|\beta|$ donc $|\alpha|-|\beta| \leqslant |\alpha+\beta|$).
$|\alpha|-|\beta| \leqslant |\alpha+\beta|$ et $|\alpha+\beta| \leqslant |\gamma|$ donc $|\alpha|-|\beta| \leqslant |\gamma|$.
$|\alpha|-|\beta| \leqslant |\gamma|$ donc $|\alpha| \leqslant |\gamma|+|\beta|$.

B] 1) $ax+b \mid n$ et $n \neq 0$ donc (par A]) $|ax| \leqslant |b|+|n|$.
$a \neq 0$ donc $|a| > 0$. $|a| > 0$ et $|a| \in \mathbb{N}$ donc $|a| \geqslant 1$.
$|a| \geqslant 1$ et $|x| \geqslant 0$ donc $|x||a| \geqslant |x|1$. D'où $|xa| \geqslant |x|$.
$|x| \leqslant |ax|$ et $|ax| \leqslant |b|+|n|$ donc $|x| \leqslant |b|+|n|$.

2) Notons $m = |b|+|n|$. $|b| \in \mathbb{N}$ et $|n| \in \mathbb{N}$ donc $|b|+|n| \in \mathbb{N}$. D'où $m \in \mathbb{N}$.
D'apres 1), $\forall x \in A\ |x| \leqslant m$ donc $\forall x \in A\ -m \leqslant x \leqslant m$ donc $\forall x \in A\ x \in \{-m, \ldots, m\}$.
$\forall x \in A\ x \in \{-m, \ldots, m\}$ donc $A \subset \{-m, \ldots, m\}$.
$A \subset \{-m, \ldots, m\}$ et $\{-m, \ldots, m\}$ est fini donc A est fini.

C] • Soit $x \in S$.
$ax+b \mid cx+d$ donc $ax+b \mid a(cx+d)$.
$ax+b \mid a(cx+d)$ et $ax+b \mid c(ax+b)$ donc $ax+b \mid a(cx+d)-c(ax+b)$. D'où $ax+b \mid ad-bc$.

• Notons $F = \{x \in \mathbb{Z} \mid\ ax+b \mid ad-bc\}$.
Par le • précédent, on a $\forall x \in S\ x \in F$. D'où $S \subset F$.
$a \neq 0$ et $ad-bc \neq 0$ donc (par B]2)) F est fini.
$S \subset F$ et F est fini donc S est fini.