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

Corrigé du contrôle terminal d'arithmétique et de cryptographie

Exercice 1.

1) • $5^{2k+1} = 5^{2k}.5^1 = (5^2)^k.5 = 25^k.5$. D'où $5^{2k+1} = 5.25^k$.
$25 = 1 + 3.8$ donc $25 \equiv 1$ [8].
$25 \equiv 1$ [8] et $k \in \mathbb{N}$ donc $25^k \equiv 1^k$ [8]. D'où $25^k \equiv 1$ [8].
$25^k \equiv 1$ [8] donc $5.25^k \equiv 5.1$ [8]. $5^{2k+1} = 5.25^k$ donc $5^{2k+1} \equiv 5$ [8].

• $3^{2k} = (3^2)^k$ donc $3^{2k} = 9^k$.
$9 = 1 + 1.8$ donc $9 \equiv 1$ [8]. $9 \equiv 1$ [8] et $k \in \mathbb{N}$ donc $9^k \equiv 1^k$ [8]. D'où $9^k \equiv 1$ [8].
$9^k \equiv 1$ [8] donc $2.9^k \equiv 2.1$ [8]. $3^{2k} = 9^k$ donc $2.3^{2k} \equiv 2$ [8].

• $5^{2k+1} \equiv 5$ [8] et $2.3^{2k} \equiv 2$ [8] donc $5^{2k+1} + 2.3^{2k} \equiv 5 + 2$ [8]. D'où $5^{2k+1} + 2.3^{2k} \equiv 7$ [8].
$5^{2k+1} + 2.3^{2k} \equiv 7$ [8] donc $(5^{2k+1} + 2.3^{2k}) + 1 \equiv 7 + 1$ [8]. D'où $5^{2k+1} + 2.3^{2k} + 1 \equiv 8$ [8].
$5^{2k+1} + 2.3^{2k} + 1 \equiv 8$ [8] et $8 \equiv 0$ [8] donc $5^{2k+1} + 2.3^{2k} + 1 \equiv 0$ [8].

• $5^{2k+1} + 2.3^{2k} + 1 \equiv 0$ [8] donc $8 \mid 5^{2k+1} + 2.3^{2k} + 1$.

2) • On a vu précédemment que $5^{2k+1} \equiv 5$ [8] donc on a $5.5^{2k+1} \equiv 5.5$ [8]. D'où $5^{2k+2} \equiv 25$ [8].
$5^{2k+2} \equiv 25$ [8] et $25 \equiv 1$ [8] (vu précédemment) donc $5^{2k+2} \equiv 1$ [8].

• On a vu précédemment que $2.3^{2k} \equiv 2$ [8] donc on a $3(2.3^{2k}) \equiv 3.2$ [8]. D'où $2.3^{2k+1} \equiv 6$ [8].

• $5^{2k+2} \equiv 1$ [8] et $2.3^{2k+1} \equiv 6$ [8] donc $5^{2k+2} + 2.3^{2k+1} \equiv 1 + 6$ [8]. D'où $5^{2k+2} + 2.3^{2k+1} \equiv 7$ [8].
$5^{2k+2} + 2.3^{2k+1} \equiv 7$ [8] donc $(5^{2k+2} + 2.3^{2k+1}) + 1 \equiv 7 + 1$ [8]. D'où $5^{2k+2} + 2.3^{2k+1} + 1 \equiv 8$ [8].
$5^{2k+2} + 2.3^{2k+1} + 1 \equiv 8$ [8] et $8 \equiv 0$ [8] donc $5^{2k+2} + 2.3^{2k+1} + 1 \equiv 0$ [8].

• $5^{2k+2} + 2.3^{2k+1} + 1 \equiv 0$ [8] donc $8 \mid 5^{2k+2} + 2.3^{2k+1} + 1$.

3) On distingue deux cas.

• On suppose n pair.
n est pair et $n \in \mathbb{N}$ donc il existe $k \in \mathbb{N}$ tel que $n = 2k$.
$k \in \mathbb{N}$ donc (par 1)) $8 \mid 5^{2k+1} + 2.3^{2k} + 1$. D'où $8 \mid 5^{n+1} + 2.3^n + 1$.

• On suppose n impair.
n est impair et $n \in \mathbb{N}$ donc il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$.
$k \in \mathbb{N}$ donc (par 2)) $8 \mid 5^{2k+2} + 2.3^{2k+1} + 1$. D'où $8 \mid 5^{n+1} + 2.3^n + 1$.

Exercice 2.

• Montrons que i) $\Longrightarrow$ ii).
On suppose que u et v sont premiers entre eux.
u et v sont premiers entre eux donc, par le théorème de Bézout, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha u + \beta v = 1$.
$\alpha u + \beta v = 1$ donc $\alpha u = 1 - \beta v$. $\alpha u = 1 + (-\beta)v$ donc $\alpha u \equiv 1$ [v].

• Montrons que ii) $\Longrightarrow$ i).
On suppose qu'il existe $\alpha \in \mathbb{Z}$ tel que $\alpha u \equiv 1$ [v].

$\alpha u \equiv 1\ [v]$ donc il existe $k \in \mathbb{Z}$ tel que $\alpha u = 1 + kv$.
$\alpha u = 1 + kv$ donc $\alpha u - kv = 1$. $\alpha u + (-k)v = 1$ donc u et v sont premiers entre eux.

Exercice 3.

1) • Montrons que $\mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta) \subset \mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d)$.
Soit $x \in \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$.
$x \in \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$ donc $x \in \mathrm{Div}(\alpha)$ et $x \in \mathrm{Div}(\beta)$.
$x \in \mathrm{Div}(\alpha)$ donc $x \mid \alpha$.
$x \in \mathrm{Div}(\beta)$ donc $x \mid \beta$.
$x \mid \alpha$ et $x \mid \beta$ donc $x \mid a\alpha + b\beta$. $x \mid \alpha a + \beta b$ donc $x \in \mathrm{Div}(\alpha a + \beta b)$.
$x \mid \alpha$ et $x \mid \beta$ donc $x \mid c\alpha + d\beta$. $x \mid \alpha c + \beta d$ donc $x \in \mathrm{Div}(\alpha c + \beta d)$.
$x \in \mathrm{Div}(\alpha a + \beta b)$ et $x \in \mathrm{Div}(\alpha c + \beta d)$ donc $x \in \mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d)$.

• Montrons que $\mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d) \subset \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$.
Soit $x \in \mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d)$.
$x \in \mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d)$ donc $x \in \mathrm{Div}(\alpha a + \beta b)$ et $x \in \mathrm{Div}(\alpha c + \beta d)$.
$x \in \mathrm{Div}(\alpha a + \beta b)$ donc $x \mid \alpha a + \beta b$.
$x \in \mathrm{Div}(\alpha c + \beta d)$ donc $x \mid \alpha c + \beta d$.

∗ $x \mid \alpha a + \beta b$ donc $x \mid d(\alpha a + \beta b)$. D'où $x \mid (ad)\alpha + (bd)\beta$.
$x \mid \alpha c + \beta d$ donc $x \mid b(\alpha c + \beta d)$. D'où $x \mid (bc)\alpha + (bd)\beta$.
$x \mid (ad)\alpha + (bd)\beta$ et $x \mid (bc)\alpha + (bd)\beta$ donc $x \mid [(ad)\alpha + (bd)\beta] - [(bc)\alpha + (bd)\beta]$
donc $x \mid (ad - bc)\alpha$. $ad - bc = 1$ donc $x \mid \alpha$ donc $x \in \mathrm{Div}(\alpha)$.

∗ $x \mid \alpha a + \beta b$ donc $x \mid c(\alpha a + \beta b)$. D'où $x \mid (ac)\alpha + (bc)\beta$.
$x \mid \alpha c + \beta d$ donc $x \mid a(\alpha c + \beta d)$. D'où $x \mid (ac)\alpha + (ad)\beta$.
$x \mid (ac)\alpha + (ad)\beta$ et $x \mid (ac)\alpha + (bc)\beta$ donc $x \mid [(ac)\alpha + (ad)\beta] - [(ac)\alpha + (bc)\beta]$
donc $x \mid (ad - bc)\beta$. $ad - bc = 1$ donc $x \mid \beta$ donc $x \in \mathrm{Div}(\beta)$.

∗ $x \in \mathrm{Div}(\alpha)$ et $x \in \mathrm{Div}(\beta)$ donc $x \in \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$.

• Concluons.
$\mathrm{Div}(\alpha a+\beta b)\cap\mathrm{Div}(\alpha c+\beta d) \subset \mathrm{Div}(\alpha)\cap\mathrm{Div}(\beta)$ et $\mathrm{Div}(\alpha)\cap\mathrm{Div}(\beta) \subset \mathrm{Div}(\alpha a+\beta b)\cap\mathrm{Div}(\alpha c+\beta d)$
donc $\mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d) = \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta)$.

2) Les assertions suivantes sont équivalentes :
i) $\alpha a + \beta b$ et $\alpha c + \beta d$ sont premiers entre eux ;
ii) α et β sont premiers entre eux.
En effet, on a les équivalences suivantes :

$$\begin{aligned} \alpha a + \beta b \text{ et } \alpha c + \beta d \text{ sont premiers entre eux} &\iff \mathrm{Div}(\alpha a + \beta b) \cap \mathrm{Div}(\alpha c + \beta d) = \{-1, 1\} \\ &\iff \mathrm{Div}(\alpha) \cap \mathrm{Div}(\beta) = \{-1, 1\} \\ &\iff \alpha \text{ et } \beta \text{ sont premiers entre eux} \end{aligned}$$

Exercice 4.

A] 1) a) p est premier et $p \nmid x$ donc p est premier avec x.
p est premier avec x donc x est premier avec p.
$x \mid pq$ et x est premier avec p donc (lemme de Gauss) $x \mid q$.

b) $x \in \mathbb{N}$ et $x \mid q$ donc $x \in \mathrm{Div}_+(q)$.
q est premier donc $\mathrm{Div}_+(q) = \{1, q\}$.
$x \in \mathrm{Div}_+(q)$ et $\mathrm{Div}_+(q) = \{1, q\}$ donc $x \in \{1, q\}$.
$x \in \{1, q\}$ donc $x = 1$ ou $x = q$.

2) p est premier donc $p \geqslant 2$ donc $p \neq 0$.
$p \mid x$ et $p \neq 0$ donc on dispose du quotient de x par p.
L'énoncé note k le quotient de x par p, on a donc $x = kp$.

a) $x = kp$ et $x \mid pq$ donc $kp \mid pq$.
$pk \mid pq$ et $p \neq 0$ donc $k \mid q$.
$x \in \mathbb{N}$, $p \in \mathbb{N}^*$ et k est le quotient de x par p donc $k \in \mathbb{N}$.
$k \in \mathbb{N}$ et $k \mid q$ donc $k \in \mathrm{Div}_+(q)$.
q est premier donc $\mathrm{Div}_+(q) = \{1, q\}$.
$k \in \mathrm{Div}_+(q)$ et $\mathrm{Div}_+(q) = \{1, q\}$ donc $k \in \{1, q\}$.
$k \in \{1, q\}$ donc $k = 1$ ou $k = q$.

b) ($k = 1$ ou $k = q$) et $x = kp$ donc $x = 1p$ ou $x = qp$ donc $x = p$ ou $x = pq$.

B] • Justifions que $\{1, p, q, pq\} \subset \mathrm{Div}_+(pq)$.
$1 \in \mathbb{N}$ et $1 \mid pq$ donc $1 \in \mathrm{Div}_+(pq)$.
$p \in \mathbb{N}$ et $p \mid pq$ donc $p \in \mathrm{Div}_+(pq)$.
$q \in \mathbb{N}$ et $q \mid pq$ donc $q \in \mathrm{Div}_+(pq)$.
$pq \in \mathbb{N}$ et $pq \mid pq$ donc $pq \in \mathrm{Div}_+(pq)$.
On en déduit que $\{1, p, q, pq\} \subset \mathrm{Div}_+(pq)$.

• Justifions que $\mathrm{Div}_+(pq) \subset \{1, p, q, pq\}$.
Soit $x \in \mathrm{Div}_+(pq)$.
$x \in \mathrm{Div}_+(pq)$ donc $x \in \mathbb{N}$ et $x \mid pq$. Donc le A] s'applique. On distingue deux cas.

∗ On suppose $p \nmid x$.
Par A]1)b), on a $x = 1$ ou $x = q$. D'où $x \in \{1, p, q, pq\}$.

∗ On suppose $p \mid x$.
Par A]2)b), on a $x = p$ ou $x = pq$. D'où $x \in \{1, p, q, pq\}$.

• Concluons.
$\mathrm{Div}_+(pq) \subset \{1, p, q, pq\}$ et $\{1, p, q, pq\} \subset \mathrm{Div}_+(pq)$ donc $\mathrm{Div}_+(pq) = \{1, p, q, pq\}$.

Exercice 5.

• On suppose $a = 0$.
On sait que $\mathbb{Z}0 = \{0\}$.
On vérifie que pour toute partie A de $\mathbb{Z}$ on a $\{0\} + A = A$. En particulier, $\{0\} + \mathbb{N} = \mathbb{N}$.
On conlut : $\mathbb{Z}0 + \mathbb{N} = \mathbb{N}$.

• On suppose $a \neq 0$.

∗ $\mathbb{Z}a + \mathbb{N} \subset \mathbb{Z}$ est connu.

∗ Vérifions que $\mathbb{Z} \subset \mathbb{Z}a + \mathbb{N}$.

Soit $b \in \mathbb{Z}$.
$a \neq 0$ donc (par division euclidienne) il existe $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tels que $0 \leqslant r < |a|$ et $b = qa + r$.
$r \in \mathbb{Z}$ et $r \geqslant 0$ donc $r \in \mathbb{N}$. $qa \in \mathbb{Z}a$ et $r \in \mathbb{N}$ donc $qa + r \in \mathbb{Z}a + \mathbb{N}$. D'où $b \in \mathbb{Z}a + \mathbb{N}$.

$*$ Concluons.
$\mathbb{Z}a + \mathbb{N} \subset \mathbb{Z}$ et $\mathbb{Z} \subset \mathbb{Z}a + \mathbb{N}$ donc $\mathbb{Z}a + \mathbb{N} = \mathbb{Z}$