karam.fayad@eisti.eu

Corrigé DS3 Algèbre (14/12/2018)

Exercice 1 .

1. $\Rightarrow$) Si x possède un inverse modulo n, alors il existe $y \in \mathbb{Z}$, $xy \equiv 1[n]$, ainsi n divise $xy-1$. Il existe donc $k \in \mathbb{Z}$, $xy-1 = nk$, d'où $xy - nk = 1$. C'est une relation de Bézout entre x et n, donc $x \wedge n = 1$.
   $\Leftarrow$) Si $x \wedge n = 1$, alors il existe $(u, v) \in \mathbb{Z}^2$, $xu + nv = 1$, ainsi $xu = 1 - nv \equiv 1[n]$. Donc u est un inverse de x modulo n.
2. (a) Si $xy_1 \equiv 1[n]$ et $xy_2 \equiv 1[n]$, alors en particulier $xy_1 \equiv xy_2[n]$, ainsi n divise $xy_1 - xy_2 = x(y_1 - y_2)$; or $x \wedge n = 1$, donc par le lemme de Gauss, n divise $y_1 - y_2$. Ainsi, $y_1 \equiv y_2[n]$.
   (b) i. On a $3 \times 2 = 6 \equiv 1[5]$, ainsi l'inverse de 3 modulo 5 est 2.
   ii. On a $4 \times (-6) = -24 \equiv 1[25]$, ainsi l'inverse de 4 modulo 25 est 19 ($19 \equiv -6[25]$).
   iii. On a $3 \times 7 = 21 \equiv 1[10]$, ainsi l'inverse de 3 modulo 10 est 7.
3. (a) Existence : Comme $a \wedge n = 1$, alors il existe $y \in \mathbb{Z}$, $ay \equiv 1[n]$ d'où $ayb \equiv b[n]$. Ainsi yb est solution.
   Unicité (modulo n) : si x_1 et x_2 sont deux solutions, alors en particulier $ax_1 \equiv ax_2[n]$, et comme $a \wedge n = 1$, on déduit que $x_1 \equiv x_2[n]$ (lemme de Gauss).
   (b) i. $2x \equiv 7[7] \Leftrightarrow 2x \equiv 0[7] \Leftrightarrow x \equiv 0[7]$
   (en utilisant que $2 \wedge 7 = 1$ pour l'implication $2x \equiv 0[7] \Rightarrow x \equiv 0[7]$).
   ii. En remarquant que 13 est l'inverse de 3 modulo 38 (car $3 \times 13 = 39 \equiv 1[38]$), on a :
   $3x \equiv 25[38] \Leftrightarrow 39x \equiv 325[38] \Leftrightarrow x \equiv 325 \equiv 21[38]$.
   (en utilisant que $38 \wedge 13 = 1$ dans l'implication $39x \equiv 325[38] \Rightarrow 3x \equiv 25[38]$).
4. (a) Si $x \equiv x_0[n_1 n_2]$, alors $n_1 n_2 | x - x_0$, en particulier $n_1 | x - x_0$ et $n_2 | x - x_0$. Ainsi, $x \equiv x_0 \equiv a_1[n_1]$ et $x \equiv x_0 \equiv a_2[n_2]$. Ainsi x est solution.
   Réciproquement, si x est solution, alors en particulier $x \equiv x_0[n_1]$ et $x \equiv x_0[n_2]$, ainsi, $x - x_0$ est un multiple commun à n_1 et n_2, c'est donc un multiple de $n_1 \vee n_2 = n_1 n_2$. D'où $x \equiv x_0[n_1 n_2]$.
   (b) Comme $n_1 \wedge n_2 = 1$, ça découle directement de la question (1).
   (c) D'après la question précédente, $n_1 y_1 \equiv 1[n_2]$ et $n_2 y_2 \equiv 1[n_1]$, d'où :
   - modulo n_1 : $a_1 n_2 y_2 + a_2 n_1 y_1 \equiv a_1 n_2 y_2 \equiv a_1[n_1]$
   - modulo n_2 : $a_1 n_2 y_2 + a_2 n_1 y_1 \equiv a_2 n_1 y_1 \equiv a_2[n_2]$
   (d) D'après les questions précédentes, les solutions du systèmes sont les entiers x qui s'écrivent $x = a_1 n_2 y_2 + a_2 n_1 y_1 + k n_1 n_2$ avec $k \in \mathbb{Z}$.
5. L'inverse de 4 modulo 9 étant 7 ($y_1 = 7$) et celui de 9 modulo 4 étant 1 ($y_2 = 1$), on déduit qu'une solution particulière du système est $3 \times 9 \times 1 + 2 \times 4 \times 7 = 83$. Les solutions dont donc les entiers x tels que $x \equiv 83[36]$ (ou de façon équivalente $x \equiv 11[36]$).

Exercice 2 .

1. $2520 = 2^3 \times 3^2 \times 5 \times 7$ et $26400 = 2^5 \times 3 \times 5^2 \times 11$, d'où $2520 \wedge 26400 = 2^3 \times 3 \times 5 = 120$.
2. (a) Effectuons l'algorithme d'Euclide :

$$\begin{aligned} 462 &= 294 \times 1 + 168 \\ 294 &= 168 \times 1 + 126 \\ 168 &= 126 \times 1 + 42 \\ 126 &= 42 \times 3 + 0 \end{aligned}$$

   Ainsi, $462 \wedge 294 = 42$ et on remontant l'algorithme d'Euclide, on obtient :

$$\begin{aligned} 42 &= 168 - 126 \\ &= 168 - (294 - 168) = 2 \times 168 - 294 \\ &= 2 \times (462 - 294) - 294 \\ &= 2 \times 462 - 3 \times 294 \end{aligned}$$

ce qui fournit une relation de Bézout.

(b) $462 \wedge 294 = 42$ divise 84, ainsi l'équation possède des solutions, et est équivalente à (en divisant par 42) : $11x + 7y = 2$. D'après la question précédente, le couple $(x_0, y_0) = (4, -6)$ est une solution.
Soit maintenant (x, y) une solution, on a a alors $11x + 7y = 11x_0 + 7y_0$, d'où $11(x - x_0) = 7(y_0 - y)$, ainsi $7|11(x - x_0)$ et par le lemme de Gauss, $7|x - x_0$. Ainsi, il existe $k \in \mathbb{Z}$, $x = x_0 + 7k = 4 + 7k$ puis $y = y_0 - 11k = -6 - 11k$.
Réciproquement, si $x = 4 + 7k$ et $y = -6 - 11k$, alors $11x + 7y = 2$.
L'ensemble des couples (x, y) solutions est donc

$$\{(4 + 7k, -6 - 11k),\ k \in \mathbb{Z}\}.$$

Exercice 3 .

1. (a) i. Soit d un diviseur positif commun à k et l. On a alors $d|k$ et $k|a$ alors $d|a$; de même, $d|l$ et $l|b$ alors $d|b$. Or $a \wedge b = 1$, d'où $d = 1$. Ainsi le seul diviseur commun positif à k et l est 1, d'où $k \wedge l = 1$.

   ii. Soit (k, l) et (k', l') deux éléments de $\mathcal{D}(a) \times \mathcal{D}(b)$ tels que $\varphi(k, l) = \varphi(k', l')$. On a alors $kl = k'l'$ d'où $k'|kl$ or $k' \wedge l = 1$ d'après la question précédente. Par le lemme de Gauss, on déduit que $k'|k$. De la même façon, on montre que $k|k'$, ainsi $k = k'$ (car la divisibilité est une relation antisymétrique sur $\mathbb{N}$).
   Comme $k = k'$, et $kl = k'l'$, on déduit que $l = l'$. (aucun de ces entiers n'est nul car $a \neq 0$ et $b \neq 0$).
   On a donc $(k, l) = (k', l')$, d'où l'injectivité de φ.

   (b) Comme $a \wedge b \neq 1$, soit $d \neq 1$ un diviseur positif commun à a et b. Ainsi, les deux couples $(d, 1)$ et $(1, d)$ sont deux éléments de $\mathcal{D}(a) \times \mathcal{D}(b)$ qui sont distincts et tels que $\varphi(d, 1) = \varphi(1, d) = d$. On en déduit que φ n'est pas injective.

   (c) D'après la question (a), on a : $a \wedge b = 1 \Rightarrow \varphi$ est injective.
   D'après la question (b), on a : $a \wedge b \neq 1 \Rightarrow \varphi$ n'est pas injective. De façon équivalente (par contraposée) : φ est injective $\Rightarrow a \wedge b = 1$.
   On déduit l'équivalence : $a \wedge b = 1 \Leftrightarrow \varphi$ est injective.

2. (a) Soit $(k, l) \in \mathcal{D}(a) \times \mathcal{D}(b)$. On a :
   Si $(k, l) \in \varphi^{-1}(\{p\})$ alors $\varphi(k, l) = kl = p$ or p est premier ainsi $(k, l) = (1, p)$ ou $(k, l) = (p, 1)$, donc $p|a$ ou $p|b$, donc $p|ab$. Absurde. On en déduit que $\varphi^{-1}(\{p\}) = \emptyset$.

   (b) D'après la question précédente, p n'a aucun antécédent par φ, ainsi φ n'est pas surjective.

3. (a) Soit $n \in \mathbb{N}$. On a :
   $n \in \varphi(\mathcal{D}(a) \times \mathcal{D}(b)) \Rightarrow \exists (k, l) \in \mathcal{D}(a) \times \mathcal{D}(b)$, $n = \varphi(k, l) = kl$. Comme $k|a$ et $l|b$, alors $kl|ab$, ainsi $n = kl \in \mathcal{D}(ab)$.

   (b) Soit maintenant $d \in \mathcal{D}(ab)$. Notons $\delta = d \wedge a$ et écrivons $d = \delta d'$, $a = \delta a'$ avec $a' \wedge d' = 1$.
   Comme $d|ab$, alors $\delta d'|\delta a'b$, alors $d'|a'b$, or $a' \wedge d' = 1$ donc $d'|b$ (par le lemme de Gauss).
   Finalement $(\delta, d') \in \mathcal{D}(a) \times \mathcal{D}(b)$ et $d = \delta d' = \varphi(\delta, d') \in \varphi(\mathcal{D}(a) \times \mathcal{D}(b))$.