Corrigé du partiel de maths discrètes

Exercice 1. a) Appliquons l'algorithme d'Euclide à $b = 47$ et $a = 26$:

$$\begin{array}{rcll} 47 & = & 1 \times 26 & + \; 21 \\ 26 & = & 1 \times 21 & + \; 5 \\ 21 & = & 4 \times 5 & + \; 1 \\ 5 & = & 5 \times 1 & + \; 0 \end{array}$$

On en déduit que a et b sont premiers entre eux. De plus,

$$\begin{aligned} 1 &= 21 - 4 \times 5 = 21 - 4 \times (26 - 21) \\ &= -4 \times 26 + 5 \times 21 = -4 \times 26 + 5 \times (47 - 26) \\ &= 5 \times 47 - 9 \times 26 \end{aligned}$$

Donc $-9a + 5b = 1$ est une relation de Bézout entre a et b.

b) L'égalité $1 + ax = 2 + by$ est équivalente à $ax - by = 1$. On vient de montrer que $x_0 = -9, y_0 = -5$ forment une solution particulière. Si (x, y) vérifie $ax - by = 1$, alors $a(x - x_0) = b(y - y_0)$. Donc b divise $a(x - x_0)$. Comme a et b sont premiers entre eux, le théorème de Gauss implique que b divise $x - x_0$, autrement dit il existe $k \in \mathbb{Z}$ tel que $x - x_0 = bk$. Ceci implique que $y - y_0 = ak$. Réciproquement, tout couple $(x, y) = (x_0 + bk, y_0 + ak)$ est solution de $ax - by = 1$.
Conclusion : l'ensemble des couples (x, y) solutions de $1+ax = 2+by$ est $\{(-9+bk, -5+ak) \mid k \in \mathbb{Z}\}$.

c) $n - 1$ multiple de $a \iff$ il existe $x \in \mathbb{Z}$ tel que $n - 1 = ax$, autrement dit $n = 1 + ax$.
$n - 2$ multiple de $b \iff$ il existe $y \in \mathbb{Z}$ tel que $n - 2 = by$, autrement dit $n = 2 + by$.
Donc $n \in \mathbb{Z}$ vérifie la propriété demandée si et seulement s'il existe des entiers x, y tels que $n = 1 + ax = 2 + by$.
L'équation $1 + ax = 2 + by$ a des solutions par b). En prenant $n = 1 + ax$, on en déduit qu'il existe des entiers relatifs n tels que $n - 1$ soit multiple de a et $n - 2$ soit multiple de b, et l'ensemble des solutions $n \in \mathbb{Z}$ est $S = \{1 - 9a + abk \mid k \in \mathbb{Z}\} = \{-233 + abk \mid k \in \mathbb{Z}\}$.

Exercice 2. a) Les décompositions en facteurs premiers de 4^n et 10^n sont : $4^n = 2^{2n}$ et $10^n = 2^n \cdot 5^n$. Donc $\mathrm{pgcd}(4^n, 10^n) = 2^n$.

b) La décomposition en facteurs premiers de 100 est $100 = 2^2 \cdot 5^2$. Puisque $\mathrm{ppcm}(a, b) = 100$, les seuls nombres premiers pouvant apparaître dans les décompositions de a et b sont 2 et 5, donc il existe des entiers naturels $\alpha_1, \alpha_2, \beta_1, \beta_2$ tels que $a = 2^{\alpha_1} \cdot 5^{\alpha_2}$ et $b = 2^{\beta_1} \cdot 5^{\beta_2}$. Les égalités $\mathrm{pgcd}(a, b) = 5$ et $\mathrm{ppcm}(a, b) = 100$ sont alors équivalentes à :
- $\min(\alpha_1, \beta_1) = 0$ et $\max(\alpha_1, \beta_1) = 2$,
- $\min(\alpha_2, \beta_2) = 1$ et $\max(\alpha_2, \beta_2) = 2$.

Il y a donc 4 couples de solutions (a, b) :
- $(a, b) = (5, 100)$ (pour $\alpha_1 = 0, \beta_1 = 2, \alpha_2 = 1, \beta_2 = 2$),
- $(a, b) = (25, 20)$ (pour $\alpha_1 = 0, \beta_1 = 2, \alpha_2 = 2, \beta_2 = 1$),
- $(a, b) = (20, 25)$ (pour $\alpha_1 = 2, \beta_1 = 0, \alpha_2 = 1, \beta_2 = 2$),
- $(a, b) = (100, 5)$ (pour $\alpha_1 = 2, \beta_1 = 0, \alpha_2 = 2, \beta_2 = 1$).

Exercice 3. a) L'équation $10x \equiv a \ (26)$ est équivalente à : $\exists k \in \mathbb{Z}$, $10x - 26k = a$. On sait que cette équation d'inconnues x, k a des solutions si et seulement si $\mathrm{pgcd}(10, 26)$ divise a. Or $10 = 2 \times 5$ et $26 = 2 \times 13$ (décomposition en facteurs premiers), donc $\mathrm{pgcd}(10, 26) = 2$. Conclusion : l'équation $10x \equiv a \ (26)$ a des solutions si et seulement si a est un entier pair.

b) L'équation $10x \equiv 4 \ (26)$ est équivalente à : $\exists k \in \mathbb{Z}$, $10x - 26k = 4$. En divisant par $2 = \mathrm{pgcd}(10, 26)$, on obtient l'équation $5x - 13k = 2$, d'inconnues x et k, avec 5 et 13 premiers entre eux.

$2 \times 13 - 5 \times 5 = 1$ est une relation de Bézout entre 13 et 5. On en déduit qu'une solution particulière est $(x_0, k_0) = (-10, -4)$. Si (x, k) est solution de $5x - 13k = 2$, alors $5(x - x_0) = 13(k - k_0)$, donc 13 divise $5(x - x_0)$. Comme 5 et 13 sont premiers entre eux, le théorème de Gauss implique que 13 divise $x - x_0$, autrement dit il existe $p \in \mathbb{Z}$ tel que $x - x_0 = 13p$. Ceci implique que $k - k_0 = 5p$. Réciproquement, tout couple $(x, k) = (x_0 + 13p, k_0 + 5p)$ est solution. On a donc obtenu l'ensemble des solutions de $5x - 13k = 2$.
L'ensemble des $x \in \mathbb{Z}$ vérifiant $10x \equiv 4$ (26) est donc $\{-10 + 13p \mid p \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \equiv 3 \ (13)\}$.
Comme $0 \leq 3 < 13$, la plus petite solution positive est $x = 3$ (c'est le reste modulo 13).

Exercice 4. a) $8 \times 2 - 15 = 1$ donc 15 et 8 sont premiers entre eux par le théorème de Bézout et $-1 \times 15 + 2 \times 8 = 1$ est une relation de Bézout entre 15 et 8.
Soit $x_0 = (-2) \times (-1) \times 15 + (-4) \times 2 \times 8 = -34$. Alors $x_0 \equiv -4$ (15) et $x_0 \equiv -2$ (8). Donc x_0 est une solution particulière du système. Par le théorème des restes chinois, l'ensemble des solutions du système est l'ensemble des $x \equiv x_0$ (8×15), c'est-à-dire $x \equiv -34$ (120).

Remarque : on peut trouver une solution particulière – ou résoudre entièrement le système – en considérant : $\exists k, k' \in \mathbb{Z},\ x = -4 + 15k = -2 + 8k'$.

b) On appelle x le nombre de minutes à partir de l'instant présent ($x > 0$ est un temps futur, $x < 0$ est un temps passé). Le bus A passe tous les temps x vérifiant $x \equiv -4$ (15) et le bus B passe tous les temps x vérifiant $x \equiv -2$ (8). Les deux bus passent donc en même temps quand x vérifie le système

$$\begin{cases} x & \equiv & -4 & (15) \\ x & \equiv & -2 & (8) \end{cases}$$

On vient de le résoudre. La question est donc de trouver la solution x avec x positif et minimal. Les x solutions vérifient $x \equiv -34 \equiv 86$ (120). Comme $0 \leq 86 < 120$, $x = 86$ est le plus petit entier positif solution.
Conclusion : les deux bus passeront en même temps pour la première fois dans 86 minutes.

Exercice 5. a) 5 est un nombre premier, donc par le théorème de Fermat, si 5 ne divise pas n alors $n^4 \equiv 1$ (5). On en déduit :
• si n n'est pas un multiple de 5, alors $n^{41} \equiv (n^4)^{10} \cdot n \equiv 1^{10} \times n \equiv n$ (5),
• si n est un multiple de 5, alors $n \equiv 0$ (5) donc $n^{41} \equiv 0$ (5).
Dans les deux cas, $n^{41} \equiv n$ (5), autrement dit, le reste modulo 5 de n^{41} est égal au reste modulo 5 de n. Ceci implique que pour tout $n \in \mathbb{N}$, $n^{41} - n$ est divisible par 5.

b) 11 est un nombre premier, donc par le théorème de Fermat, si 11 ne divise pas n alors $n^{10} \equiv 1$ (11). Donc, si n n'est pas multiple de 11, $n^{41} - n \equiv (n^{10})^4 \cdot n - n \equiv 1^4 \times n - n \equiv 0$ (5). Et si n est multiple de 11, $n \equiv 0$ (11) donc $n^{41} - n \equiv 0$ (11). Donc pour tout $n \in \mathbb{N}$, $n^{41} - n$ est divisible par 11.

c) 5 et 11 sont premiers entre eux (car ce sont des nombres premiers distincts), et ils divisent tous les deux $n^{41} - n$ par les questions a) et b). Par le corollaire du théorème de Gauss, on en déduit que, pour tout $n \in \mathbb{N}$, $5 \times 11 = 55$ divise $n^{41} - n$.

Exercice 6. On a utilisé 11 caisses, donc 10 caisses sont pleines et contiennent n pots, et la 11ème caisse contient r pots avec $1 \leq r \leq n$. On a : $365 = 10n + r$. On écrit la division euclidienne de r par 10 : il existe $q, r' \in \mathbb{Z}$ tels que $r = 10q + r'$ et $0 \leq r' < 10$. On a alors $365 = 10(n + q) + r'$. Comme $0 \leq r' < 10$, ceci est la division euclidienne de 365 par 10 donc, par unicité du quotient et du reste, $n + q = 36$ et $r' = 5$. Ceci peut s'écrire : $\begin{cases} n & = & 36 - q \\ r & = & 10q + 5 \end{cases}$
Les valeurs possibles de n et r sont toutes les solutions de ce système avec $1 \leq r \leq n$. Si $q < 0$ alors $r < 0$ donc ce n'est pas une solution. Si $q \geq 3$ alors $n \leq 33$ et $r \geq 35 > n$ donc ce n'est pas une solution non plus. Il y a finalement 3 couples solutions, pour $0 \leq q \leq 2$:
• $n = 36$ et $r = 5$ (pour $q = 0$),
• $n = 35$ et $r = 15$ (pour $q = 1$),
• $n = 34$ et $r = 25$ (pour $q = 2$).