DM d'Arithmétique : corrigé

(1) *Montrez que pour tout $n \in \mathbb{Z}$, il existe un unique couple $(\lambda, \mu) \in \mathbb{Z}^2$ tel que $n = \lambda a + \mu b$ et $0 \leq \lambda \leq b - 1$.*

Prouvons l'existence. D'après le théorème de Bézout, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $ua + vb = 1$. En multipliant par n, on trouve $nua + nvb = n$. Effectuons la division euclidienne de nu par b et notons λ le reste. On obtient $nu = qb + \lambda$ avec $0 \leq \lambda \leq b - 1$, et de plus

$$nua + nvb = (qb + \lambda)a + nvb = \lambda a + (qa + nv)b \; .$$

Ainsi, si l'on pose $\mu = qa + nv$, on a bien $n = \lambda a + \mu b$ avec $0 \leq \lambda \leq b - 1$.

L'unicité est vérifiée par le même argument que celui qui donne l'unicité du couple (quotient,reste) dans le division euclidienne (cf votre cours). Précisément, s'il existe deux couples (λ, μ) et (λ', μ') satisfaisant les conditions demandées, alors $n = \lambda a + \mu b = \lambda' a + \mu' b$. On en déduit que $(\lambda - \lambda')a = (\mu' - \mu)b$. Posons $x := \lambda' - \lambda$, on a ainsi : b divise xa, or b est premier avec a donc par le lemme de Gauss, b divise x.

Comme de plus λ et λ' sont tous deux dans $\{0, \dots, b-1\}$ on a $|x| = |\lambda - \lambda'| \leq b - 1 < b$. Comme x est un multiple de b, ceci n'est possible que si $x = 0$. Donc $\lambda' = \lambda$, et on en déduit facilement que $\mu' = \mu$.

(2) *Décrire en termes mathématiques l'ensemble des bons prix.*

L'ensemble des bons prix est l'ensemble des nombres qui s'écrivent $\lambda a + \mu b$ avec λ et μ entiers naturels, ou plus formellement $\{n \in \mathbb{N}\,,\, \exists (\lambda, \mu) \in \mathbb{N}^2, n = \lambda a + \mu b\,\}$. En particulier, il est clair que la somme de 2 bons prix est un bon prix.

(3) *Pour chaque couple (a, b) d'entiers premiers entre eux tels que $2 \leq a < b \leq 7$, faire la liste des mauvais prix.*

(4) *Soit m le plus grand mauvais prix (présumé) dans les onze exemples ci-dessus. Pour chaque couple (a, b), indiquer les valeurs de m et de $m + a + b$. Pouvez-vous proposer une formule $m = f(a, b)$ donnant le plus grand mauvais prix ?*

a	b	Ensemble des mauvais prix	m	$m+a+b$
2	3	$\{1\}$	1	6
2	5	$\{1;3\}$	3	10
2	7	$\{1;3;5\}$	5	14
3	4	$\{1;2;5\}$	5	12
3	5	$\{1;2;4;7\}$	7	15
3	7	$\{1;2;4;5;8;11\}$	11	21
4	5	$\{1;2;3;6;7;11\}$	11	20
4	7	$\{1;2;3;5;6;9;10;13;17\}$	17	28
5	6	$\{1;2;3;4;7;8;9;13;14;19\}$	19	30
5	7	$\{1;2;3;4;6;8;9;11;13;16;18;23\}$	23	35
6	7	$\{1;2;3;4;5;8;9;10;11;15;16;17;22;23;29\}$	29	42

Sur ces exemples, on constate que l'ensemble des mauvais prix est fini.

De plus, sur ces exemples toujours, $m + a + b$ est toujours égal à ab. On peut donc poser $f(a, b) := ab - (a + b)$ et se demander si la formule $m = f(a, b)$ est vraie en général.

(5) *Démontrez cette formule en deux étapes : d'abord montrez que $f(a, b)$ n'est pas un bon prix, ensuite, montrez que tout prix $n > f(a, b)$ est un bon prix.*

Démontrons que $f(a, b) = ab - (a + b)$ est un mauvais prix. Supposons que $ab - (a + b)$ soit un bon prix, c'est-à-dire qu'il existe $(\lambda, \mu) \in \mathbb{N}^2$ tels que $ab - (a + b) = \lambda a + \mu b$. On en déduit $ab = (\lambda + 1)a + (\mu + 1)b$. Ainsi a divise $(\mu + 1)b$ donc, comme a et b sont premiers entre eux, par le lemme de Gauß on obtient que a divise $\mu + 1$. De même, on montre que b divise $\lambda + 1$:

$$\exists \mu' \in \mathbb{N},\ \mu + 1 = \mu' a$$
$$\exists \lambda' \in \mathbb{N},\ \lambda + 1 = \lambda' b$$

On a donc $ab = \lambda' ab + \mu' ab$ d'où en divisant par ab : $1 = \lambda' + \mu'$. Nécessairement, $\lambda' = 0$ ou $\mu' = 0$ (sinon leur somme serait au moins égale à 2). Cela implique alors que $\lambda + 1 = \lambda' b = 0$ (si $\lambda' = 0$) ou que $\mu + 1 = \mu' a = 0$ (si $\mu' = 0$). C'est impossible puisque $\lambda \geq 0$ et $\mu \geq 0$. Cela signifie donc que $ab - (a + b)$ est un mauvais prix.

Démontrons ensuite que tout prix $p \geq f(a, b) + 1$ est un bon prix. Soit donc $p \in \mathbb{N}$ tel que $p \geq ab - (a + b) + 1$. Considérons l'écriture de Bézout unique $p = \lambda a + \mu b$ avec $0 \leq \lambda \leq b - 1$. Montons qu'on a alors $\mu \geq 0$. En effet, sinon on a $\mu \leq -1$ donc

$$p = \lambda a + \mu b \leq (b - 1)a - b = ab - a - b$$

or on a supposé le contraire. Donc $p = \lambda a + \mu b$ avec $\lambda \geq 0$ et $\mu \geq 0$, c'est-à-dire que p est un bon prix.

La conclusion est que le plus grand mauvais prix est $m = ab - (a + b)$, en particulier, il n'y a qu'un nombre fini de mauvais prix.

(6) *Montrez que m est impair.*

On a $m = (a - 1)(b - 1) - 1$. Comme a et b sont premiers entre eux, l'un au moins est impair. Donc $a - 1$ ou $b - 1$ est pair, donc $(a - 1)(b - 1)$ est pair. Donc $m = (a - 1)(b - 1) - 1$ est impair.

Une autre démonstration vient en raisonnant modulo 2. Comme a et b sont premiers entre eux on ne peut pas avoir $a \equiv 0\ (2)$ et $b \equiv 0\ (2)$. Donc on a trois possibilités :

(i) $a \equiv 0$ et $b \equiv 1$. Dans ce cas $ab - (a + b) \equiv 0 - (0 + 1) \equiv -1 \equiv 1$.

(ii) $a \equiv 1$ et $b \equiv 0$. Dans ce cas $ab - (a + b) \equiv 0 - (1 + 0) \equiv -1 \equiv 1$.

(iii) $a \equiv 1$ et $b \equiv 1$. Dans ce cas $ab - (a + b) \equiv 1 - (1 + 1) \equiv -1 \equiv 1$.

Dans tous les cas on voit que $ab - (a + b)$ est congru à 1 modulo 2, i.e. est impair.

(7) *On sait maintenant qu'il n'y a qu'un nombre fini de mauvais prix ; on veut les compter. Soit E l'ensemble $\{0, 1, \ldots, m\}$. Montrez que la fonction $i \colon E \to E$ définie par $i(x) = m - x$ échange les mauvais prix et les bons prix.*

On doit montrer que, étant donné $p \in E = \{0, 1, \ldots, m\}$, si p est un bon prix alors $m - p$ est un mauvais prix, et si p est un mauvais prix alors p est un bon prix.

Supposons que p est un bon prix. Si $m-p$ était aussi un bon prix, alors la somme $p+(m-p) = m$ serait un bon prix (voir (2)). Ceci n'est pas vrai. Donc, $m - p$ est un mauvais prix.

Supposons maintenant que p est un mauvais prix et montrons que $m - p$ est un bon prix. Considérons l'écriture de Bézout unique de $m - p$, c'est-à-dire $m - p = \lambda a + \mu b$ avec $(\lambda, \mu) \in \mathbb{Z}^2$ et $0 \leq \lambda \leq b - 1$. Il suffit de montrer qu'alors $\mu \geq 0$. Or, on a

$$p = m - (m - p) = m - (\lambda a + \mu b) = ab - (a + b) - (\lambda a + \mu b) = (b - (\lambda + 1))a - (\mu + 1)b$$

Posons $\lambda' := b - (\lambda + 1)$ et $\mu' := -(\mu + 1)$, de sorte que $p = \lambda' a + \mu' b$. Vu qu'on a choisi l'écriture de Bézout unique on a $\lambda' \geq 0$, si de plus $\mu' \geq 0$ alors p serait un bon prix, contrairement à l'hypothèse. Ainsi, $\mu' < 0$ i.e. $\mu \geq 0$ qui est ce qu'on voulait montrer. Donc $m - p$ est un bon prix.

(8) *Déduisez-en le nombre de mauvais prix.*

L'ensemble $E = \{0, 1, \ldots, m\}$ compte $m + 1 = (a - 1)(b - 1)$ éléments. Or, la fonction i est bijective (sa réciproque est elle-même !) et envoie le sous-ensemble des bons prix sur le sous-ensemble des mauvais prix. Donc elle partage E en deux parties de même cardinal. Ainsi, il y a $\frac{1}{2}(a - 1)(b - 1)$ mauvais prix.

(9) *Vérifiez le résultat sur les exemples du tableau.*

Le nombre de mauvais prix pour chaque colonne du tableau est : 1, 2, 3, 3, 4, 6, 6, 9, 10, 12, 15. Cela correspond bien à $\frac{1}{2}(a - 1)(b - 1)$, dans chaque cas.

(10) *Trouver tous les couples (a, b) d'entiers naturels premiers entre eux tels que le nombre de mauvais prix soit égal à 26.*

On doit chercher des couples (a, b) d'entiers premiers entre eux et tels que $\frac{1}{2}(a-1)(b-1) = 26$. Cela équivaut à $(a - 1)(b - 1) = 52$. Donc $a - 1$ et $b - 1$ sont des diviseurs de 52, soit, 1, 2, 4, 13, 26, ou 52. Supposons que $a \leq b$, les possibilités sont

(i) $a - 1 = 1$ et $b - 1 = 52$.

(ii) $a - 1 = 2$ et $b - 1 = 26$.

(iii) $a - 1 = 4$ et $b - 1 = 13$.

Le cas (ii) est à exclure car $a = 3$ et $b = 27$ ne sont pas premiers entre eux. Il reste les couples $(a, b) = (2, 53)$ et $(5, 14)$ (lorsque $a \leq b$) et $(53, 2)$ et $(14, 5)$ (lorsque $a > b$).