Compter les mauvais prix

Supposons être dans un pays où il n'y a que deux types de pièces de monnaie, disons des pièces de a€ et b€, avec a et b premiers entre eux. Alors, d'après le théorème de Bézout, on peut payer en espèces tous les montants entiers, en demandant au besoin aux commerçants de rendre la monnaie. Si les commerçants ne rendent pas la monnaie, il y a des *mauvais prix* qu'on ne peut pas payer exactement.

Théorème *Le nombre de mauvais prix est fini et égal à* $\frac{1}{2}(a-1)(b-1)$.

Pour la preuve, nous utiliserons l'*écriture de Bézout unique* suivante : pour tout entier $n \in \mathbb{Z}$ il existe un couple unique $(\lambda, \mu) \in \mathbb{Z}^2$ tel que $n = \lambda a + \mu b$ avec $0 \leq \lambda \leq b-1$. On l'obtient immédiatement en prenant une écriture de Bézout quelconque et en faisant la division euclidienne de λ par b.

Lemme 1 *Le plus grand mauvais prix est* $m = ab - (a+b)$.

Preuve : Démontrons que $ab-(a+b)$ 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 mauvais prix n vérifie $n \leq ab-(a+b)$. Considérons l'écriture de Bézout unique $n = \lambda a + \mu b$ avec $0 \leq \lambda \leq b-1$. Comme c'est un mauvais prix on doit avoir $\mu \leq -1$ et donc $n = \lambda a + \mu b \leq (b-1)a - b = ab - a - b$. □

Lemme 2 *Soit* $E = \{0, 1, \ldots, m\}$. *Alors, l'involution* $i \colon E \to E$ *définie par* $i(x) = m - x$ *échange les mauvais prix et les bons prix.*

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

Supposons maintenant que x est un mauvais prix et montrons que $m-x$ est un bon prix. Considérons l'écriture de Bézout unique de $m-x$, c'est-à-dire $m-x = \lambda a + \mu b$ 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

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

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

La conclusion du théorème est maintenant évidente. □