Solutions positives des équations diophantiennes

Daniel PERRIN

1 Introduction

Si p et q sont des entiers premiers entre eux, une conséquence du théorème de Bézout est que tout entier n peut s'écrire sous la forme $n = ap + bq$, voir par exemple [ME] Ch. 1, §3.g. Une question plus difficile est de savoir, lorsque p, q et n sont positifs [1], si l'on peut écrire n avec des coefficients a, b positifs (ou positifs ou nuls). C'est souvent important dans les applications, notamment les récréations, voir par exemple le problème 99 de [ME] dont voici un extrait :

Le maire de Saint-Tricotin-sur-Pelote (Marne-et-Garonne) a décidé de quitter la zone euro et de faire utiliser aux habitants de Saint-Tricotin leur propre monnaie : la maille. Pour éviter de frapper trop de sortes de pièces, deux types de pièces seulement seront disponibles, l'une de 9 mailles, l'autre de 11 mailles.

Au début de l'opération, les commerçants n'ont pas de pièces pour rendre la monnaie et les acheteurs doivent faire l'appoint. Faire la liste des sommes ≤ 30 *mailles que l'on peut payer. Peut-on payer les sommes suivantes (en mailles) :* 41, 53, 71, 79 *? Montrer qu'on peut payer n'importe quelle somme* $c \geq 99$ *mailles (on suppose que l'acheteur a à sa disposition autant de pièces qu'il veut). Indiquer toutes les manières de payer 118 mailles, 417 mailles.*

Le texte [2] ci-dessous fait le point sur ce problème dans le cas de deux entiers et donne une application dans le cas de trois.

2 Le résultat pour deux entiers

Le théorème ci-dessous règle les deux cas des coefficients > 0 ou ≥ 0 :

2.1 Théorème. *Soient p, q des entiers positifs premiers entre eux.*

1) Tout entier $n > pq$ s'écrit sous la forme $n = ap + bq$ avec $a, b > 0$. Le nombre pq n'est pas de cette forme.

2) Tout entier $n > pq - p - q$ s'écrit sous la forme $n = ap + bq$ avec $a, b \geq 0$. Le nombre $pq - p - q$ n'est pas de cette forme.

1. On utilise ici ce mot au sens de > 0.

2. Je remercie vivement Olivier Dupuy de m'avoir posé cette question au début de l'année scolaire 2012-2013, puis de m'avoir rappelé, à la fin de la même année, alors que je me reposais la question, que j'y avais répondu ! La vieillesse est un naufrage ...

Démonstration. 1) On écrit une relation de Bézout quelconque $\lambda p + \mu q = 1$ avec $\lambda, \mu \in \mathbf{Z}$, qui donne $n = \lambda np + \mu nq$. On sait (voir [ME] *loc. cit.*) qu'alors les solutions a, b de l'équation $ap + bq = n$ sont de la forme $a = \lambda n + kq$ et $b = \mu n - kp$, avec $k \in \mathbf{Z}$, et il s'agit de trouver k de sorte que a et b soient > 0. Cela donne les conditions $-\dfrac{\lambda n}{q} < k < \dfrac{\mu n}{p}$ et il reste à voir s'il existe toujours un entier dans l'intervalle, ce qui est assuré si la différence des bornes est > 1. On trouve donc la condition $\big(\dfrac{\mu}{p} + \dfrac{\lambda}{q}\big)n = \dfrac{(\lambda p + \mu q)n}{pq} = \dfrac{n}{pq} > 1$, c'est-à-dire $n > pq$.

Si l'on a $pq = ap + bq$ on voit que b est multiple de p, $b = pb'$, et on en déduit $q = a + qb'$, ce qui est absurde si a et b (donc aussi b') sont positifs.

2) Il reste à attraper les n de la zone intermédiaire. Un tel n s'écrit $pq - p - q + k$ avec $1 \leq k \leq p + q$. On a donc $pq + k > pq$ et, par le point précédent, il s'écrit $pq + k = ap + bq$ avec $a, b > 0$, donc $a, b \geq 1$. Mais alors on a $n = pq - p - q + k = (a - 1)p + (b - 1)q$, avec $a - 1, b - 1 \geq 0$.

Si l'on a $pq - p - q = ap + bq$ avec $a, b \geq 0$ on en déduit $pq = (a+1)p + (b+1)q$ et cela contredit le premier point.

2.2 *Remarque.* Dans le problème de Saint-Tricotin, on peut donc payer, sans rendre la monnaie, n'importe quelle somme $> 79 = 9 \times 11 - 9 - 11$ mailles.

3 Application dans le cas de trois entiers

3.1 Le cas de Z

Rappelons d'abord le résultat avec les coefficients entiers relatifs :

3.1 Théorème. *Soient $p, q, r \in \mathbf{Z}$ des entiers*[3] *premiers entre eux. Pour tout $n \in \mathbf{Z}$ il existe $a, b, c \in \mathbf{Z}$ tels que $ap + bq + cr = n$.*

Démonstration. Bien entendu, il suffit de traiter le cas $n = 1$. Posons $d = pgcd(p, q)$. Par hypothèse d est premier avec r. On écrit d'abord $d = a'p + b'q$, puis $1 = \lambda d + cr$, le tout par Bézout. On en déduit $1 = \lambda a'p + \lambda b'q + cr$.

3.2 Le cas de N

3.2.1 Existence

On suppose maintenant $p, q, r > 0$ (et par exemple $p \leq q \leq r$). Pour l'heure, je n'ai pas de résultat définitif dans ce cas. Voici un résultat partiel :

3. Cette expression signifie qu'il n'existe aucun entier autre que ± 1 qui divise à la fois p, q, r. Une condition plus forte est que p, q, r soient deux à deux premiers entre eux.

3.2 Théorème. *Soient p, q, r des entiers > 0 premiers entre eux. On pose $M_{p,q} = pgcd(p,q)r + ppcm(p,q)$ et de même avec q, r et p, r et on appelle M le minimum de ces trois nombres. Alors, tout entier $n > M$ (resp. $n > M - p - q - r$) s'écrit sous la forme $n = ap + bq + cr$ avec $a, b, c > 0$ (resp. $a, b, c \geq 0$).*

Démonstration. Supposons par exemple $n > M_{p,q}$. Posons $d = pgcd(p,q)$, on a donc $p = dp'$ et $q = dq'$ avec p' et q' premiers enture eux et $m := ppcm(p,q) = dp'q'$. Comme r est premier avec d, il existe $c \in \{1, 2, \ldots, d\}$ tel que $n - cr \equiv 0 \pmod{d}$. Posons $n' = (n - cr)/d$. On a $n > dr + m = dr + dp'q' \geq cr + dp'q'$, donc $n' > p'q'$. En vertu de 2.1, il existe $a, b > 0$ tels que $n' = ap' + bq'$, donc $n - cr = ap + bq$ et on a le résultat.

Le cas des inégalités larges en résulte. Si l'on a $n > M - p - q - r$, donc $n + p + q + r > M$, on peut écrire $n + p + q + r = ap + bq + cr$ avec $a, b, c \geq 1$. On a donc $n = (a-1)p + (b-1)q + (c-1)r$ avec $a - 1, b - 1, c - 1 \geq 0$.

3.3 *Remarques.* 1) Si p, q, r sont pemiers entre eux deux à deux et si l'on a $p \leq q \leq r$ on vérifie qu'on a $M_{p,q} = r + pq \leq M_{q,r} = q + pr \leq M_{q,r} = p + qr$, de sorte que le minimum M est égal à $M_{p,q}$. Si les nombres ne sont pas deux à deux premiers entre eux, en revanche, on ne peut affirmer que le minimum M est égal à $M_{p,q}$, même si l'on suppose $p < q < r$. Par exemple, pour $p = 9$, $q = 11$ et $r = 21$, on a $M_{p,q} = 21 + 99 = 120$ mais $M_{p,r} = 33 + 63 = 96 < 120$.

2) **Attention**, le nombre M n'est pas en général optimal, il se peut que des nombres $< M$ soient de la forme $ap + bq + cr$ avec $a, b, c > 0$. Voici un exemple : $p = 3$, $q = 5$, $r = 7$, le nombre M est égal à $M_{p,q}$ c'est-à-dire à 22. Pourtant on atteint non seulement 22, mais encore 21 et 20, de sorte que le dernier entier n non atteint avec des coefficients positifs est 19.

3) Si N est le plus grand entier qui ne s'écrit pas $ap + bq + cr$ avec $a, b, c > 0$, il est clair que $N - p - q - r$ est le plus grand entier qui ne s'écrit pas $ap + bq + cr$ avec $a, b, c \geq 0$.

3.2.2 Optimalité

Voici un résultat partiel en ce sens :

3.4 Théorème. *Soient p, q, r des entiers > 0 premiers entre eux. Soit $d = pgcd(p,q)$, $m = ppcm(p,q)$, $M = M_{p,q} = dr + m$. On écrit $p = dp'$, $q = dq'$ avec p', q' premiers entre eux et on suppose $r > p'q' - p' - q'$. Alors, M n'est pas de la forme $ap + bq + cr$ avec $a, b, c > 0$ (donc M est le plus grand nombre qui n'est pas de cette forme).*

Démonstration. Supposons $M = dr+m = ap+bq+cr$. On a donc $dr+dp'q' = adp'+bdq'+cr$. Comme r et d sont premiers entre eux, le théorème de Gauss montre que d divise c, $c = dc'$. On en déduit $p'q' = ap' + bq' + (c'-1)r$ avec $a', b', c' > 0$. Le cas $c' = 1$ est exclu en vertu de 2.1. On a donc $c' - 1 \geq 1$ d'où $r \leq p'q' - ap' - bq' \leq p'q' - p' - q'$ et c'est impossible par hypothèse.

3.5 *Remarques.* 1) Le cas $3, 5, 7$ est exactement dans la situation limite : $7 = 3 \times 5 - 3 - 5$, on a vu que la valeur $M = 22$ n'est pas optimale.

2) Plus généralement, avec les notations de 3.4, on vérifie que, si r est égal à $p'q' - p' - q'$, $M = dr + m$ est de la forme $ap + bq + cr$ avec $a = b = 1$ et $c = 2d$. Dans ce cas, la valeur M n'est pas optimale.

3) Attention cependant, si r est plus petit que $p'q' - p' - q'$, il se peut cependant que $M_{p,q}$ soit optimal. Par exemple, avec $p = 5$, $q = 7$ et $r = 22$, on a $M = 57$ et ce nombre n'est pas de la forme $5a+7b+22c$ avec $a, b, c > 0$. Bref, la situation est plus compliquée qu'il n'y paraît de prime abord !

3.3 Une application

3.6 Théorème. *Tout entier $n > 210$ (resp > 139) s'écrit sous la forme $n = 15a + 21b + 35c$ avec $a, b, c > 0$ (resp. ≥ 0) et ces bornes sont optimales.*

Démonstration. On a $M = M_{p,q} = 3 \times 35 + 3 \times 5 \times 7 = 210$ et $M - p - q - r = 139$, ce qui assure l'existence des écritures en vertu de 3.2. Avec les notations de 3.4 on a $d = 3$, $p' = 5$, $q' = 7$ et $r = 35 > p'q' - p' - q'$, d'où l'optimalité.

4 Référence

[ME] PERRIN Daniel, *Mathématiques d'École*, Cassini (2011) (deuxième édition).