Fatale erreur

Patrick David (daiweide1@gmail.com)

Mars 2023

Énoncé abrégé : Au fil des problèmes 547-2 (AFDM 547, p 71)

Soient $(b, q, r) \in \mathbb{R}_+^{*3}$, montrer que l'on peut trouver une infinité de (b, q, r) tels que $bq + r = (b + q)r \quad (1)$ avec $0 < r < b$

I Résolution

Un paramétrage intéressant de ce problème s'obtient en posant $b = r + k$ avec $1 \leq k$. L'équation (1) devient :

$$(r + k)q + r = (r + k + q)r \Leftrightarrow q = \frac{r(r + k - 1)}{k} = \frac{r(r - 1)}{k} + r \quad (2)$$

Théorème 1: Il existe une infinité (dénombrable) de triplets d'entiers naturels non nuls (n, q, r) tels que la division euclidienne $n = bq+r$ puisse s'écrire faussement $n = (b+q)r$

Démonstration : Dans l'expression (2) il suffit que $\frac{r(r-1)}{k}$ soit entier. Ceci est en particulier réalisé de manière triviale pour quatre familles infinies de solutions paramétrées par k ou r :

1. Si r=1, on a alors immédiatement $q = 1$ et donc $b = n - 1$. On trouve alors les solutions particulières :
   Pour $n = 3$, r=1 et $b = n - 1 = 2 : 3 = 2 \times 1 + 1$= $(2 + 1)\times 1$
   Pour $n = 4$, r=1 et $b = n - 1 = 3 : 4 = 3 \times 1 + 1$= $(3 + 1)\times 1$
   Pour $n = 5$, r=1 et $b = n - 1 = 4 : 5 = 4 \times 1 + 1$= $(4 + 1)\times 1$
   .....
   Pour n , r=1 et $b = n - 1 : n = (n - 1) \times 1 + 1$= $((n - 1) + 1)\times 1$

2. Si r quelconque et $k = 1$. On trouve les solutions particulières :

   Pour $r = 1$, $k = 1$ et $b = r + 1 = 2 : 3 = 2 \times 1 + 1$= $(2 + 1)\times 1$
   Pour $r = 2$, $k = 1$ et $b = r + 1 = 3 : 14 = 3 \times 4 + 2$= $(3 + 4)\times 2$
   Pour $r = 3$, $k = 1$ et $b = r + 1 = 4 : 39 = 4 \times 9 + 3$= $(4 + 9)\times 3$
   Pour $r = 4$, $k = 1$ et $b = r + 1 = 5 : 84 = 5 \times 16 + 4$= $(5 + 16)\times 4$
   .....
   Pour r , $k = 1$ et $b = r + 1 : n = b \times q + r$= $(b + q)\times r$

3. Si r quelconque et $k = r$. On trouve les solutions particulières :
   Pour $r = 1$, $k = 1$ et $b = r + k = 2r = 2 : 3 = 2 \times 1 + 1 = (\ 2 + 1\ ) \times 1$
   Pour $r = 2$, $k = 2$ et $b = r + k = 2r = 4 : 14 = 4 \times 3 + 2 = (\ 4 + 3\ ) \times 2$
   Pour $r = 3$, $k = 3$ et $b = r + k = 2r = 6 : 33 = 6 \times 5 + 3 = (\ 6 + 5\ ) \times 3$
   Pour $r = 4$, $k = 4$ et $b = r + k = 2r = 8 : 60 = 8 \times 7 + 4 = (\ 8 + 7\ ) \times 4$
   .....
   Pour r , $k = r$ et $b = r + k = 2r : n = b \times q + r = (\ b + q\ ) \times r$

4. Si r quelconque et $k = r - 1$. On trouve les solutions particulières :
   Pour $r = 2$, $k = 1$ et $b = r + k = 2r - 1 = 3 : 14 = 3 \times 4 + 2 = (\ 3 + 4\ ) \times 2$
   Pour $r = 3$, $k = 2$ et $b = r + k = 2r - 1 = 5 : 33 = 5 \times 6 + 3 = (\ 5 + 6\ ) \times 3$
   Pour $r = 4$, $k = 3$ et $b = r + k = 2r - 1 = 7 : 60 = 7 \times 8 + 4 = (\ 7 + 8\ ) \times 4$
   Pour $r = 5$, $k = 4$ et $b = r + k = 2r - 1 = 9 : 95 = 9 \times 10 + 5 = (\ 9 + 10\ ) \times 5$
   .....
   Pour r , $k = r - 1$ et $b = r + k = 2r - 1 : n = b \times q + r = (\ b + q\ ) \times r$

On remarque que l'on retrouve les mêmes résultats au débuts de ces différents cas, et que les cas 3 et 4 sont les mêmes, sauf avec $r = 1$, avec le rôle de b et de q qui sont échangés. Le seul cas où b et k ne peuvent pas être échangés provient de la condition $r < b$ alors que cette contrainte n'est pas valide pour q.

II Retour sur Bézout

Si on a bien prouvé qu'il y avait une infinité de solutions pour les équations (1) et(2), les trois familles de solutions ne contiennent pas tous les cas possibles. L'exemple simple : $64 = 10 \times 6 + 4 = (10 + 6) \times 4$, pour lequel $r = 6$ et $k = 4$ n'entre dans aucune de ses trois familles. En effet, on a simplifié la fraction $\frac{r(r-1)}{k} + r$ en choisissant soit $k = 1$, soit $k = r$ soit $k = r - 1$.
Pour la suite des calculs, nous avons besoin du théorème de Bézout et de précisions sur le couple de Bézout d'un couple d'entiers premiers entre eux.
Théorème de Bézout — Soit un couple d'entiers relatifs non nuls (u, v). u et v sont premiers entre eux si et seulement s'il existe un couple d'entiers relatifs (α, β) tel que $\alpha u + \beta v = 1$.
On appelle (α, β) un couple de Bézout du couple (u, v) d'entiers premiers entre eux.
Remarque : 1. Ce couple n'est pas unique, car pour tout entier relatif γ, si (α, β) est un couple de Bézout du couple (u, v), alors $\alpha + \gamma v, \beta - \gamma u$ est un autre couple de Bézout de (u, v). En effet $(\alpha + \gamma v)u + (\beta - \gamma u)v = \alpha u + \beta v = 1$.
Remarque : 2. Si (u, v) est un couple d'entiers naturels non nuls, premier entre eux, alors tous les couples de Bézout (α, β) de (u, v) sont tels que $\alpha \times \beta < 0$. Il- est évident que si (α, β) sont de même signe, l'égalité à 1 est impossible.
Remarque : 3. Si (u, v) est un couple d'entiers naturels non nuls, premier entre eux, il existe une infinité de couples de Bézout (α, β) avec $\alpha > 0$ et $\beta < 0$. On appellera ces couples des **couples de Bézout standard** de (u, v).
Remarque : 4. Parmi les couples de Bézout standard du couple d'entiers naturels (u, v), il existe un unique couple (α, β)appelé le **couple standard minimal** tel que $0 < \alpha < v$. De plus, si (α, β) est le **couple standard minimal**, $\alpha_\gamma = \alpha + \gamma v$ est une suite arithmétique

de $\mathbb{N}$ de raison v non nulle.

III Recherche de toutes les solutions de (1)

Ici on suppose que $r > 1$ (cas particulier déjà vu) et donc que $r, r-1$ sont des entiers naturels non nuls et premiers entre eux. Une simplification de $\frac{r(r-1)}{k}$ plus générale doit être envisagée en posant $k = k'k''$, tel que k' divise r et k'' divise $r-1$. Comme r et $r-1$ sont premiers entre eux, il doit en être de même de k' et k''. Le cas général doit donc être tel que $k = k'k''$ en choisissant k' et k'' diviseurs de k, éventuellement égaux à 1 ou à k, mais sans facteurs premiers communs. Cela implique que la décomposition en facteurs premiers de k' et de k'' contient des facteurs premiers distincts.

On doit donc avoir $r = \alpha k'$, mais $r - 1 = \beta k'' = \alpha k' - 1$.

On constate que $\beta k'' = \alpha k' - 1 \Leftrightarrow \alpha k' - \beta k'' = 1$. Le couple (α, β) d'entiers strictement positifs existe , puisque k' et k'' sont premiers entre eux et que $(\alpha, -\beta)$ est un couple de coefficients de Bézout **standard** de (k', k''). On a donc un algorithme pour engendrer des solutions de (2) autres que les cas triviaux déjà vus.

Algorithme A :

1. Déterminer un entier $k > 1$ et déterminer sa décomposition en facteurs premiers $k = p_1^{a_1} \dots p_s^{a_s}$.
2. Partitionner l'ensemble $\{p_1^{a_1}, \dots, p_s^{a_s}\}$ en deux sous-ensembles complémentaires. Le produit de chacun des éléments de ces sous-ensembles donne respectivement k' et k'' avec $k = k'k''$ et (k', k'') sont premiers entre eux. Si une des parties est vide, le k' (ou k'') correspondant vaut 1.
3. Avec l'algorithme d'Euclide déterminer le couple de Bézout **standard minimal** $(\alpha, -\beta)$ avec $0 < \alpha < k''$. Tous les **couples de Bézout standard** sont donc $(\alpha + \gamma k'', -\beta - \gamma k')$ avec $\gamma \in \mathbb{N}$
4. Prendre $r = (\alpha + \gamma k'')k'$. En déduire $b = k + r$, $q = \frac{r(r-1)}{k} + r$ et enfin $n = bq + r$.

Théorème 2: Tous les triplets solution de l'équation (1) s'obtiennent avec l'algorithme précédent.

Démonstration : Si (b, q, r) dont tels que $n = bq + r = (b + q)r$, la première égalité vérifiant les conditions de la division euclidienne de l'entier n par b, on peut trouver $k = b - r$. $q = \frac{r(r-1)}{k} + r$ est un entier et donc k divise $r(r-1)$.
On a donc une factorisation unique $k = k'k''$ avec (k', k'') premiers entre eux, et $r = \alpha k'$, $r - 1 = \beta k''$. $(\alpha, -\beta)$ est un couple de Bézout pour (k', k''), et r, α, β correspondent à des coefficients apparaissant dans l'algorithme A.

Remarque : 5. Pour un $k = p_1^{a_1} \dots p_m^{a_m}$, l'ensemble $E = \{p_1^{a_1}, \dots, p_m^{a_m}\}$ a 2^m parties. Pour chacune des paires composées d'une partie et de son complémentaire dans E on aura en faisant les produits 2^m familles de solutions générées par ce k.

IV Exemple de constructions de familles de solutions

L'exemple non trivial le plus simple est de prendre $k = 6$ et de déterminer les 2^2 familles de solutions obtenues avec $(k', k'') \in \{(1, 6), (2, 3), (3, 2), (6, 1)\}$. Pour chaque famille on donne les deux premiers termes correspondant à $\gamma = 0$ (**couple standard minimal**), et $\gamma = 1$.

$(k', k'') = (6, 1)$ correspond au cas trivial 2 de la partie I.

(k',k")=(6, 1) ; (α , β) = (1 , -5) ; $\gamma = 0$; r = 6 ; b=r+k = 12 ; q= 11
n = b × q + r= (b + q) × r = 138 = 12 × 11 + 6 = (12 + 11) × 6

(k',k")=(6, 1) ; (α , β) = (2 , -11) ; $\gamma = 1$; r = 12 ; b=r+k = 18 ; q= 34
n = b × q + r= (b + q) × r = 624 = 18 × 34 + 12 = (18 + 34) × 12

et $(k', k'') = (1, 6)$ correspond au cas trivial 3 de la partie I.

(k',k")=(1, 6) ; (α , β) = (1 , 0) ; $\gamma = 0$; r = 1 ; b=r+k = 7 ; q= 1
n = b × q + r= (b + q) × r = 8 = 7 × 1 + 1 = (7 + 1) × 1

(k',k")=(1, 6) ; (α , β) = (7 , -1) ; $\gamma = 1$; r = 7 ; b=r+k = 13 ; q= 14
n = b × q + r= (b + q) × r = 189 = 13 × 14 + 7 = (13 + 14) × 7

Si $(k', k'') = (2, 3)$

(k',k")=(2, 3) ; (α , β) = (2 , -1) ; $\gamma = 0$; r = 4 ; b=r+k = 10 ; q= 6
n = b × q + r= (b + q) × r = 64 = 10 × 6 + 4 = (10 + 6) × 4

(k',k")=(2, 3) ; (α , β) = (5 , -3) ; $\gamma = 1$; r = 10 ; b=r+k = 16 ; q= 25
n = b × q + r= (b + q) × r = 410 = 16 × 25 + 10 = (16 + 25) × 10

Si $(k', k'') = (3, 2)$

(k',k")=(3, 2) ; (α , β) = (1 , -1) ; $\gamma = 0$; r = 3 ; b=r+k = 9 ; q= 4
n = b × q + r= (b + q) × r = 39 = 9 × 4 + 3 = (9 + 4) × 3

(k',k")=(3, 2) ; (α , β) = (3 , -4) ; $\gamma = 1$; r = 9 ; b=r+k = 15 ; q= 21
n = b × q + r= (b + q) × r = 324 = 15 × 21 + 9 = (15 + 21) × 9

Il est intéressant de vérifier que $(k', k'') = (2, 3)$ et $(k', k'') = (3, 2)$ donnent chacun une famille de solutions différente.
Si k est grand et si le nombre de facteurs premiers de k augmente, la taille des termes trouvés et le nombre de familles différentes augmentent beaucoup. Voici par exemple les deux premiers résultats pour une des familles obtenue pour $k = 60$ avec $(k', k'') = (12, 5)$ (on donne encore les deux premiers termes). Pour $k = 60 = 2^2 \times 3 \times 5$ il y a $2^3 = 8$ familles de solutions !

(k',k")=(12, 5) ; (α , β) = (3 , -7) ; $\gamma = 0$; r = 36 ; b=r+k = 96 ; q= 57
n = b × q + r= (b + q) × r = 5508 = 96 × 57 + 36 = (96 + 57) × 36

(k',k")=(12, 5) ; (α , β) = (8 , -19) ; $\gamma = 1$; r = 96 ; b=r+k = 156 ; q= 248
n = b × q + r= (b + q) × r = 38784 = 156 × 248 + 96 = (156 + 248) × 96

Les calculs et les affichages des solutions en Latex ont été obtenus avec *Mathematica*.