BROUILLON - ALGORITHME D'EUCLIDE ET COEFFICIENTS DE BACHET-BÉZOUT POUR LES HUMAINS

CHRISTOPHE BAL

Document, avec son source LaTeX, disponible sur la page
https://github.com/bc-writing/drafts.

Mentions « légales »

Table des matières

1. Où allons-nous ?

Un résultat classique d'arithmétique dit qu'étant donné $(a\,;b) \in \mathbb{N}^* \times \mathbb{N}^*$, il existe $(u\,;v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $au + bv = \text{pgcd}(a\,;b)$. Les entiers u et v seront appelés *« coefficients de Bachet-Bézout »*. Notons qu'il n'y a pas unicité car nous avons par exemple :

$$(-3) \times 12 + 1 \times 42 = 4 \times 12 + (-1) \times 42 = 6 = \text{pgcd}(12\,;42)$$

Nous allons voir comment trouver de tels entiers u et v tout d'abord de façon humainement rapide puis ensuite via des algorithmes efficaces pour un ordinateur.

2. L'algorithme « human friendly » appliqué de façon magique

2.1. Un exemple complet façon *« diaporama »*. Sur le lieu de téléchargement de ce document se trouve un fichier `PDF` de chemin relatif `bezout-coef-for-human/slide-version.pdf` présentant la méthode sous la forme d'un diaporama. Nous vous conseillons de le regarder avant de lire les explications ci-après.

Date: 10 Sept. 2019 - 13 Sept. 2019.

2.2. **Phase 1 – Au début était l'algorithme d'Euclide...** Pour chercher des coefficients de Bachet-Bézout pour $(a\,;b) = (27\,;141)$, on commence par appliquer l'algorithme d'Euclide « *verticalement* » comme suit.

$$\begin{array}{c} 141 \\[2em] 27 \end{array}$$

Étape 1 : le plus grand naturel est mis au-dessus.

$$\begin{array}{c} \boxed{141} \\[2em] \boxed{27} \end{array}$$

Étape 2 : deux naturels à diviser.

$$\begin{array}{ccc} & \boxed{141} & \\[2em] \boxed{5} & \boxed{27} & \boxed{141 = 5 \times 27 + 6} \\[2em] & \boxed{6} & \end{array}$$

Étape 3 : première division euclidienne.

$$\begin{array}{cc} & 141 \\[2em] 5 & \boxed{27} \\[2em] & \boxed{6} \end{array}$$

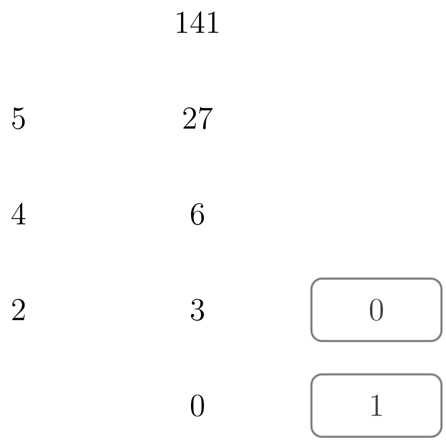
Étape 4 : on passe aux deux naturels suivants.

En répétant ce processus, nous arrivons à la représentation suivante où nous n'avons pas besoin de garder la trace des divisions euclidiennes.

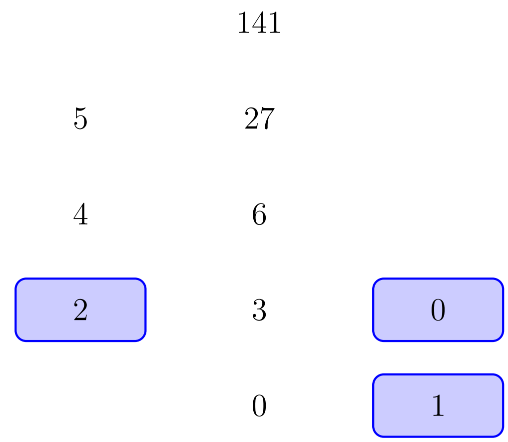
$$\begin{array}{cc} & 141 \\[2em] 5 & 27 \\[2em] 4 & 6 \\[2em] 2 & 3 \\[2em] & 0 \end{array}$$

Étape finale (1re phase) : l'algorithme d'Euclide « vertical ».

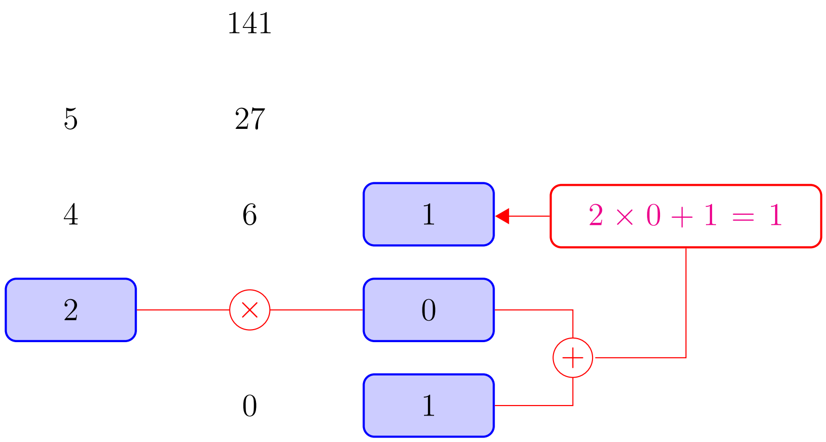
2.3. **Phase 2 – Remontée facile des étapes.** La méthode classique consiste à remonter les calculs. Mais comment faire cette remontée tout en évitant un claquage neuronal ? L'astuce est la suivante.



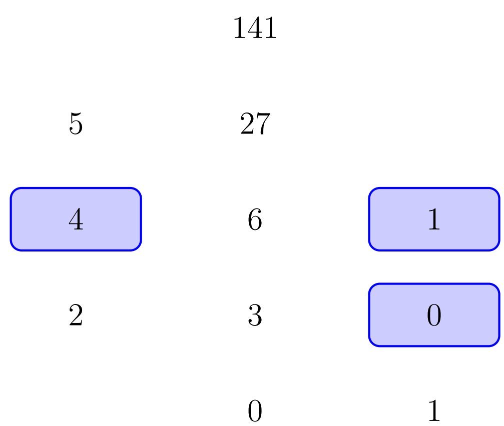
Étape 1 : ajout d'une nouvelle colonne.



Étape 2 : on n'utilise pas la colonne centrale.



Étape 3 : on fait une sorte de division « inversée ».



Étape 4 : on passe aux trois naturels suivants.

En répétant ce processus, nous arrivons à la représentation suivante.

$$\begin{array}{ccc}
 & 141 & 21 \\
5 & 27 & 4 \\
4 & 6 & 1 \\
2 & 3 & 0 \\
 & 0 & 1
\end{array}$$

Étape finale (2e phase) : remontée en voie libre des calculs.

2.4. Et voilà comment conclure !

$$\begin{array}{ccc}
 & 141 & 21 \\
5 & 27 & 4 \\
4 & 6 & 1 \\
2 & 3 & 0 \\
 & 0 & 1
\end{array}
\qquad \longrightarrow \qquad \boxed{141 \times 4 - 21 \times 27 = -3}$$

Étape finale (la vraie) : on finit avec un produit en croix.

Des coefficients de Bachet-Bézout s'obtiennent sans souci via l'équivalence suivante où nous avons $3 = \mathrm{pgcd}(27, 141)$.

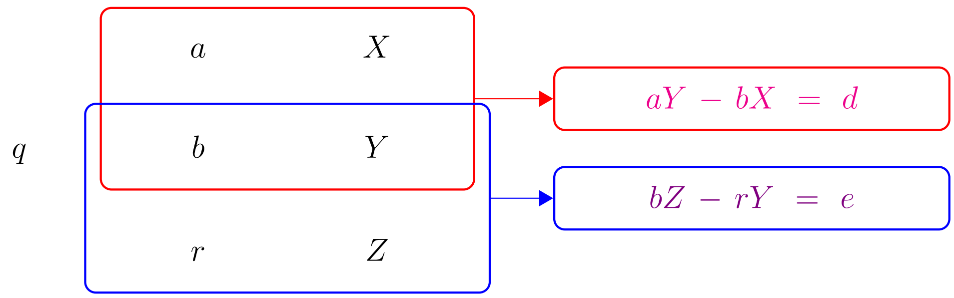
$$141 \times 4 - 27 \times 21 = -3 \iff 27 \times 21 - 141 \times 4 = 3$$

Nous allons voir, dans la section qui suit, que l'on obtient forcément à la fin $\pm\mathrm{pgcd}(27, 141)$.

En pratique, nous n'avons pas besoin de détailler les calculs comme nous l'avons fait à certains moments afin d'expliquer comment procéder. Avec ceci en tête, on comprend toute l'efficacité de la méthode présentée, mais pas encore justifiée, car il suffit de garder une trace minimale, mais complète, des étapes tout en ayant à chaque étape des opérations assez simples à effectuer. Il reste à démontrer que notre méthode marche à tous les coups. Ceci est le propos de la section suivante.

3. Pourquoi cela marche-t-il ?

3.1. Avec des arguments élémentaires. Commençons par une preuve explicative qui malheureusement ne nous permet pas de voir d'où vient l'astuce *(nous explorerons ceci dans la sous-section suivante).*



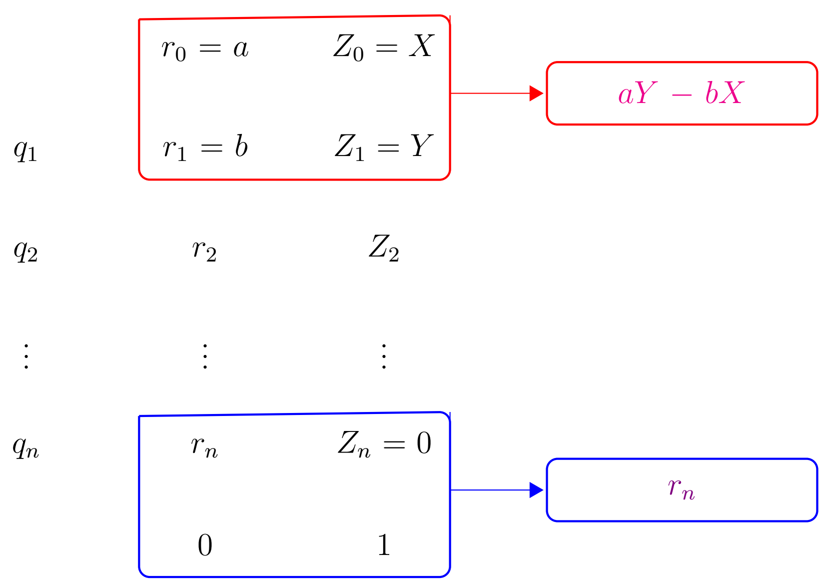
Calculs faits dans les deux phases.

Par construction, nous avons $a = qb + r$ et $X = qY + Z$. Ceci nous donne :

$$\begin{aligned} d &= aY - bX \\ &= (qb + r)Y - b(qY + Z) \\ &= rY - bZ \\ &= -e \end{aligned}$$

Donc si l'on fait « *glisser* » des carrés sur les deux colonnes de droite, les produits en croix dans ces carrés ne différeront que par leur signe.

La représentation symbolique « *complète* » ci-dessous donne $aY - bX = \pm\operatorname{pgcd}(a\,;b)$ car le dernier reste non nul de l'algorithme d'Euclide est $\operatorname{pgcd}(a\,;b)$. Ceci prouve la validité de la méthode dans le cas général. On comprend au passage l'ajout initial du 0 et du 1 dans la 3e colonne *(bien entendu,* (-1) *aurait aussi pu convenir).*



Représentation symbolique au complet.

3.2. **Avec des matrices pour y voir plus clair.** Oublions tout ce que nous avons vu précédemment. Soit $(a\,;b) \in \mathbb{N}^* \times \mathbb{N}^*$ avec $a > b$. Nous cherchons $(u\,;v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $au + bv = \operatorname{pgcd}(a\,;b)$. La petite astuce est de noter que $au + bv = \det M$ où $M = \begin{pmatrix} a & -v \\ b & u \end{pmatrix}$.

Nous allons poser $X = -v$ et $Y = u$ de sorte que $M = \begin{pmatrix} a & X \\ b & Y \end{pmatrix}$ et raisonner en supposant l'existence de u et v[1].

Soit ensuite $a = qb + r$ la division euclidienne de a par b. L'algorithme d'Euclide nous fait alors travailler avec $(b\,;r)$ au lieu de $(a\,;b)$. Comme $r = a - qb$, on peut considérer la matrice $N = \begin{pmatrix} a - qb & X - qY \\ b & Y \end{pmatrix}$ qui vérifie $\det N = \det M$ puis, afin d'avoir b en haut, la matrice $P = \begin{pmatrix} b & Y \\ a - qb & X - qY \end{pmatrix}$ qui vérifie $\det P = -\det M$.

Notant $Z = X - qY$, de sorte que $P = \begin{pmatrix} b & Y \\ r & Z \end{pmatrix}$, nous avons $X = Z + qY$. Ceci justifie la construction utilisée lors de la phase de remontée.

Pour passer à une nouvelle preuve, notons que $\begin{pmatrix} b & Y \\ r & Z \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \cdot \begin{pmatrix} a & X \\ b & Y \end{pmatrix}$ puis introduisons les notations suivantes.

- $r_0 = a$, $r_1 = b$, $Z_0 = X$ et $Z_1 = Y$ où Z_0 et Z_1 ne sont pas connus pour le moment.
- Pour $k \in \mathbb{N}^*$, on note $r_{k-1} = r_k q_k + r_{k+1}$ la division euclidienne de r_{k-1} par r_k, puis ensuite on pose $Z_{k+1} = Z_{k-1} - Z_k q_k$ de sorte que $Z_{k-1} = Z_k q_k + Z_{k+1}$.
- On note enfin $M_k = \begin{pmatrix} r_k & Z_k \\ r_{k+1} & Z_{k+1} \end{pmatrix}$ pour $k \in \mathbb{N}$ et $Q_k = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}$ pour $k \in \mathbb{N}^*$ de sorte que nous avons $M_{k+1} = Q_{k+1} \cdot M_k$ pour $k \in \mathbb{N}$. Il est immédiat que Q_k est inversible d'inverse $R_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$ avec $\det R_k = -1$.

L'algorithme d'Euclide nous donne l'existence de $n \in \mathbb{N}$ un indice minimal tel que $r_{n+1} = 0$ et $r_n = \operatorname{pgcd}(a\,;b)$.

Comme $M_n = \prod_{k=n}^{1} Q_k \cdot M_0$, nous avons $M_0 = \prod_{k=1}^{n} R_k \cdot M_n$ avec $M_0 = \begin{pmatrix} r_0 & Z_0 \\ r_1 & Z_1 \end{pmatrix} = \begin{pmatrix} a & X \\ b & Y \end{pmatrix}$ et $M_n = \begin{pmatrix} r_n & Z_n \\ 0 & Z_{n+1} \end{pmatrix} = \begin{pmatrix} \operatorname{pgcd}(a\,;b) & Z_n \\ 0 & Z_{n+1} \end{pmatrix}$.

Comme $\det M_0 = \pm 1 \det M_n$ car $\det R_k = -1$, il suffit de choisir $Z_{n+1} = 1$, avec Z_n quelconque, pour avoir $aY - bX = \pm \operatorname{pgcd}(a\,;b)$. Voilà comment découvrir la méthode visuelle vue précédemment où le choix particulier $Z_n = 0$ simplifie les tous premiers calculs.

Remarque 1. *Comme Z_n peut être quelconque, nous pouvons produire une infinité de coefficients de Bachet-Bézout. Cele vient du fait que les étapes de* « remontée » *sont du type $Z_{k-1} = Z_k q_k + Z_{k+1}$ toujours avec $q_k > 0$.*

---

4. AFFAIRE À SUIVRE...

---

1. Ce n'est qu'à la fin de la preuve que nous aurons effectivement prouver l'existence de u et v.