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 »

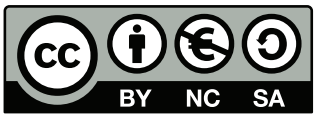


Table des matières

Date: 11 Septembre 2019.

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

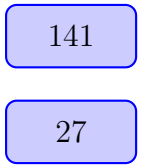
2.1. Un exemple complet façon *« diaporama »*.

Sur le lieu de téléchargement de ce document se trluve 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 suivantes.

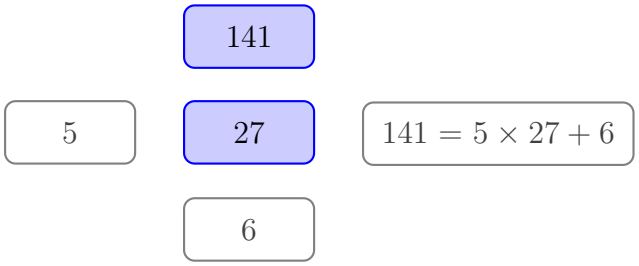
2.2. Phase 1 – Au début était l'algorithme d'Euclide.

Pour chercher des coefficients de Bachet-Bézoutpour $(a\,;b) = (27\,;141)$, on commence par appliquer l'algorithme d'Euclide *« verticalement »* comme suit.

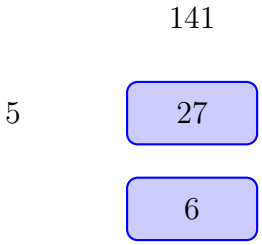
Étape 1 : le plus grand naturel est mis au-dessus.



Étape 2 : deux naturels à diviser.



Étape 3 : première division euclidienne.



Étape 4 : on passe aux deux naturels suivants.

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

	141
5	27
4	6
2	3
	0

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

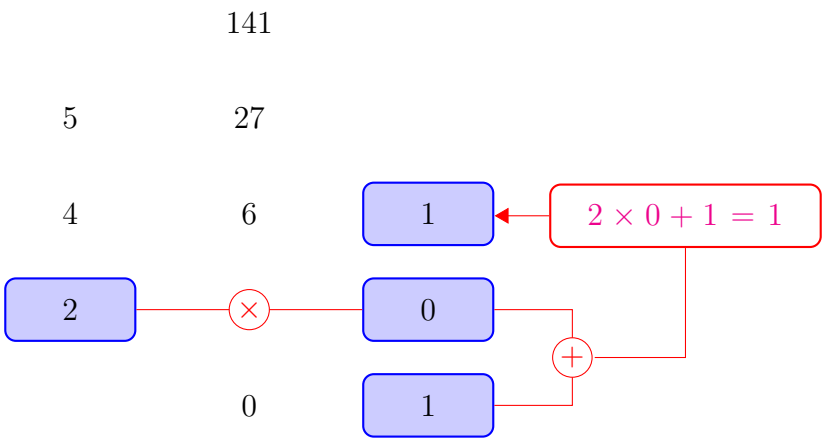
2.3. **Phase 2 – Remonter facile des étapes.** La méthode classique consiste à remonter les calculs. Mais comment faire cette remontée tout en évitant un claquage neuronal ? L'astuce est la suivante.

	141	
5	27	
4	6	
2	3	0
	0	1

Étape 1 : ajout d'une nouvelle colonne.

	141	
5	27	
4	6	
2	3	0
	0	1

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



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

	141	
5	27	
4	6	1
2	3	0
	0	1

Étape 4 : on passe aux trois naturels suivants.

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

	141	21
5	27	4
4	6	1
2	3	0
	0	1

Étape finale (2e phase) : remontée à mains nues des calculs.

2.4. **Et voilà comment conclure !**

	141	21
5	27	4
4	6	1
2	3	0
	0	1

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

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

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

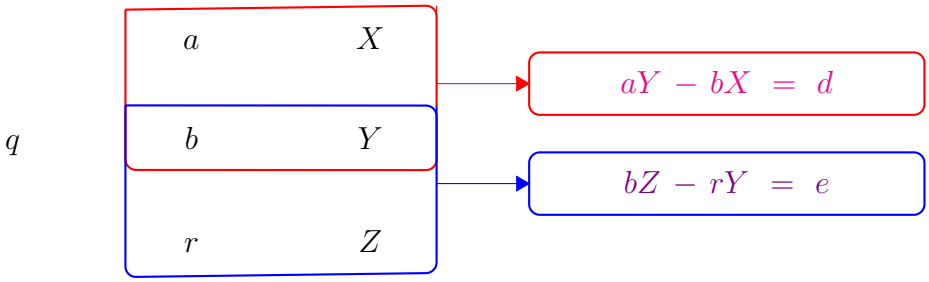
$$141 \times 4 - 27 \times 21 = -3 \iff 27 \times 21 - 141 \times 4 = 3$$

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

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)*.



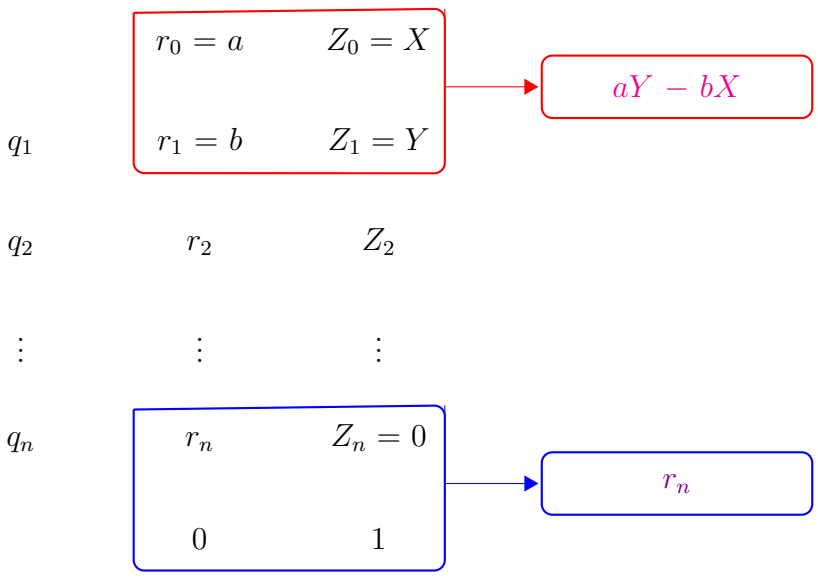
Calculs faits dans les deux phases.

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

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

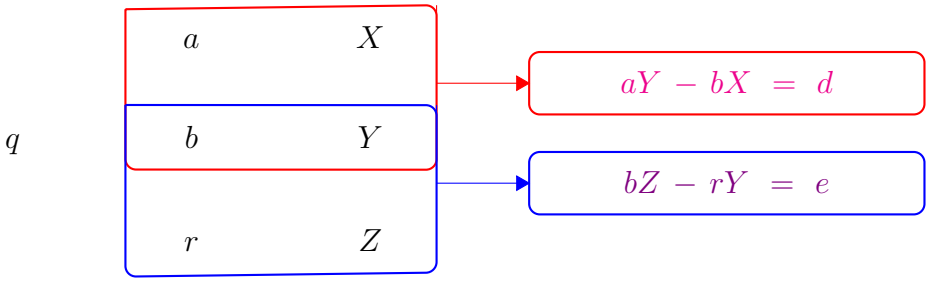
Donc si l'on fait *« glisser »* des carrés sur les deux colonnes de gauche, les produits en croix dans ces carrés ne différeront que de leur signe.

Grâce à la représentation finale ci-dessous, nous obtenons $aY - bX = \pm\,\text{pgcd}(a\,;b)$ car le dernier reste non nul de l'algorithme d'Euclide est $\text{pgcd}(a\,;b)$. 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 3$^{\text{e}}$ colonne *(bien entendu,* (-1) *aurait aussi pu convenir)*.



Une représentation symbolique au complet.

3.2. **Avec des matrices pour aller plus loin.** Reprenons le cas de base suivant mais an l'analysant à l'aune des matrices.



Calculs faits dans les deux phases.

Notant $M = \begin{pmatrix} a & X \\ b & Y \end{pmatrix}$, et $N = \begin{pmatrix} b & Y \\ r & Z \end{pmatrix}$, nous avons $d = \det M$ et $e = \det N$.

Comme

4. AFFAIRE À SUIVRE...