Algorithme d'Euclide

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Sud, France

1. Division euclidienne : École élémentaire

Soit $\mathbb{Z}$ l'anneau des nombres entiers naturels positifs ou négatifs, et soit $\mathbb{N} = \mathbb{Z}_+ \subset \mathbb{Z}$ le sous-ensemble des entiers qui sont positifs.

Définition 1.1. Diviser *avec reste* un entier $a \geqslant 1$ par un entier $1 \leqslant b \leqslant a$ qui lui est inférieur, cela consiste à trouver un *quotient* entier $q \geqslant 0$ et un *reste* entier $r \geqslant 0$ tels que :

$$a \,=\, q\,b + r,$$

le quotient q étant maximal possible, de telle sorte que dans le reste r, on ne puisse plus extraire « du b » :

$$0 \leqslant r \leqslant b - 1.$$

Il est bien connu que diviser avec reste est toujours possible, le couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ étant alors déterminé de manière unique en partant de $a \geqslant 1$ et de b avec $1 \leqslant b \leqslant a$ quelconques.

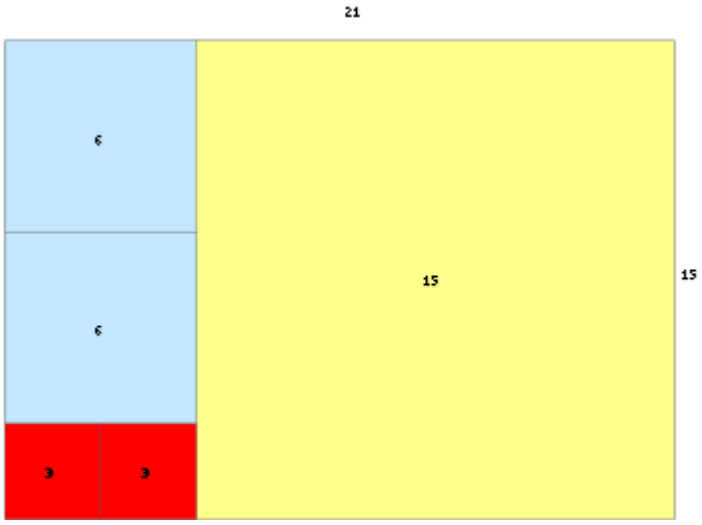
Exemple 1.2. Comme à l'école élémentaire, soit à diviser $a = 126$ par $b = 35$:

$$\begin{array}{r|l} 126 & 35 \\ \cline{2-2} -\,105 & 3 \\ 21 & \end{array}$$

Mentalement, on essaie de multiplier 35 successivement par 1, 2, 3, 4, et on trouve que $3 \times 35 = 105$ est le résultat maximum qui demeure inférieur à 126. On reporte alors $-\,105$ à gauche, on soustrait $126 - 105 = 21$, et on trouve :

$$\underbrace{126}_{a} \,=\, \underbrace{3}_{q} \cdot \underbrace{35}_{b} + \underbrace{21}_{r}.$$

Cet exemple s'inscrit dans un contexte général, connu depuis la Préhistoire sur Terre, sur Mars, sur Jupiter, sur Vénus, et sans doute aussi sur quelques exoplanètes dotées de mathématiques encore embryonnaires.



Théorème 1.3. [Division euclidienne des entiers] *Étant donné deux nombres entiers positifs quelconques $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ avec $1 \leqslant b \leqslant a$, il existe toujours un entier positif unique $q \in \mathbb{N}^*$ et un entier positif unique $r \in \mathbb{N}$ — parfois égal à 0 — tels que :*

$$\boxed{a \,=\, q\,b + r} \qquad \text{et} \qquad \boxed{0 \leqslant r < b} \qquad \square$$

Exercice 1. En s'inspirant de la figure située à droite du portrait d'Euclide, expliquer en quoi la division possède un sens géométrique.

2. Division euclidienne : polynômes à coefficients entiers

La division euclidienne fonctionne de manière essentiellement analogue dans l'anneau $\mathbb{Z}[x]$ des polynômes à une indéterminée x et à coefficients entiers, sachant que *plusieurs* opérations de soustraction successives s'avèrent nécessaires.

Exemple 2.1. Soit le polynôme quartique :

$$A(x) \,:=\, \mathbf{3\,x^4} + 2\,x^3 + x + 5,$$

à *diviser avec reste* par le polynôme quadratique (donc de degré inférieur) :

$$B(x) \,:=\, \mathbf{x^2} + 2\,x + 3,$$

les deux *monômes de tête* de A et de B étant placés en première position. On se convainc mentalement que c'est la multiplication par le monôme $3\,x^2$ qui permet de faire monter le monôme de tête de $B(x)$ à ce nouveau niveau de celui de $A(x)$:

$$\mathbf{3\,x^4} \,=\, 3\,x^2 \cdot \mathbf{x^2},$$

et donc, on est conduit à soustraire :

$$A(x) \underbrace{-\,3\,x^2\,B(x)}_{-3x^4-6x^3-9x^2},$$

procédé que l'on peut aussi représenter agréablement sous forme d'un tableau incomplet qui commence à se remplir :

$$\begin{array}{rl} 3\,x^4 + 2\,x^3 + \;0\; + x + 5 & \big|\; \underline{x^2 + 2\,x + 3} \\ -\,3\,x^4 - 6\,x^3 - 9\,x^2 & \big|\; 3\,x^2 \\ \hline -\,4\,x^3 - 9\,x^2 + x + 5 & \big| \end{array}$$

De cette manière, on fait apparaître le reste intermédiaire :

$$-\,\mathbf{4\,x^3} - 9\,x^2 + x + 5,$$

qui possède un nouveau monôme de tête $-\,\mathbf{4\,x^3}$, de telle sorte que c'est maintenant le monôme multiplicateur :

$$-\,4\,x$$

qui permet de faire remonter le monôme de tête $\mathbf{x^2}$ de $B(x)$ au niveau $-\,\mathbf{4\,x^3}$.

Après itération et épuisement de ces calculs, le tableau final s'écrit :

$$\begin{array}{rl|l}
3\,x^4 + 2\,x^3 + 0 + x + 5 & & x^2 + 2\,x + 3 \\
\cline{3-3}
-\,3\,x^4 - 6\,x^3 - 9\,x^2 & & 3\,x^2 \\
\cline{1-1}
-\,4\,x^3 - 9\,x^2 + x + 5 & & \\
4\,x^3 + 8\,x^2 + 12\,x & & -\,4\,x \\
\cline{1-1}
-\,x^2 + 13\,x + 5 & & \\
x^2 + 2\,x + 3 & & -\,1 \\
\cline{1-1}
\boxed{\mathbf{15\,x + 8}} & & \\
\cline{3-3}
& & \boxed{\mathbf{3\,x^2 - 4\,x - 1}}
\end{array}$$

Ce tableau synoptique permet alors de lire instantanément le quotient et le reste dans la division du polynôme $A(x)$ par le polynôme $B(x)$:

$$A(x) \;=\; \underbrace{\mathbf{Q(x)}}_{\text{quotient}} \cdot B(x) + \underbrace{\mathbf{R(x)}}_{\text{reste}},$$

équation qui s'écrit donc explicitement :

$$3\,x^4 + 2\,x^3 + x + 5 \;=\; \big(\mathbf{3\,x^2 - 4\,x - 1}\big) \cdot \big(x^2 + 3\,x + 3\big) + \mathbf{15\,x + 8}.$$

Bien entendu, ce deuxième exemple simple suggère aussi un procédé général, probablement déjà connu du lecteur-étudiant.

3. Division euclidienne : polynômes à coefficients dans un anneau

Afin d'embrasser la division euclidienne dans un cadre algébrique adapté, nous travaillerons maintenant avec un *anneau commutatif :*

$$\big(\mathscr{A},\, +,\, \times\big),$$

possédant un élément unité $1 \in \mathscr{A}$ pour la multiplication :

$$1 \cdot r = r \cdot 1 = r \qquad\qquad (\forall\, r \in \mathscr{A}),$$

la multiplication étant souvent notée « $\cdot$ » à la place de « $\times$ », voire même sous-entendue en omettant tout symbole.

Définition 3.1. Un élément $u \in \mathscr{A}$ est appelé une *unité* s'il existe $u' \in \mathscr{A}$ tel que :

$$u\,u' = u'\,u = 1,$$

et le groupe (multiplicatif, commutatif) des unités de $\mathscr{A}$ est alors noté $\mathscr{A}^{\times}$.

Soit maintenant x un symbole qui désigne une indéterminée. L'espace vectoriel des polynômes à coefficients dans $\mathscr{A}$:

$$\mathscr{A}[x] \,:=\, \Big\{ a_n\, x^n + a_{n_1}\, x^{n-1} + \cdots + a_1\, x + a_0 \colon\ n \in \mathbb{N},\ a_n, a_{n-1}, \ldots, a_1, a_0 \,\in\, \mathscr{A} \Big\},$$

est à nouveau un anneau commutatif possédant la même unité $1 \in \mathscr{A}$ (exercice de révision mentale).

Supposons temporairement pour simplifier que les polynômes :

$$B(x) \,=\, \mathbf{b_m}\, \mathbf{x^m} + b_{m-1}\, x^{m-1} + \cdots + b_0 \qquad\qquad (m \geqslant 0),$$

par lesquels on cherche à diviser d'autres polynômes :

$$A(x) \,=\, \mathbf{a_n}\, \mathbf{x^n} + a_{n-1}\, x^{n-1} + \cdots + a_0 \qquad\qquad (n \geqslant 0),\ ,$$

de degré supérieur $n \geqslant m$ ont toujours un coefficient de tête $\mathbf{b_m} \in \mathscr{A}^\times$ qui est une *unité*.

Définition 3.2. Étant donné un polynôme de degré $k \geqslant 0$:

$$P(x) \,=\, \mathbf{c_k}\, \mathbf{x^k} + c_{k-1}\, x^{k-1} + \cdots + c_0 \qquad\qquad (c_k \neq 0),$$

on appelle *monôme de tête* de P son terme de plus haut degré et on le note :

$$\mathsf{Tete}\big(P(x)\big) \,=\, \mathbf{c_k}\, \mathbf{x^k}.$$

Algorithme: Division polynomiale avec reste

• **Entrées :** Deux polynômes

$$A(x) \,=\, \sum_{0 \leqslant i \leqslant n} a_i\, x^i \qquad\qquad \text{et} \qquad\qquad B(x) \,=\, \sum_{0 \leqslant j \leqslant m} b_j\, x^j$$

à coefficients $a_i \in \mathscr{A}$ et $b_j \in \mathscr{A}$ de degrés respectifs $n \geqslant m \geqslant 1$ tels que le coefficient $b_m \in \mathscr{A}^\times$ du monôme de tête $\mathbf{b_m}\, \mathbf{x^m}$ de $B(x)$ est une *unité* de l'anneau $\mathscr{A}$.

• **Sorties :** Un polynôme-quotient $Q \in \mathscr{A}[x]$ et un polynôme-reste $R \in \mathscr{A}[x]$ satisfaisant :

$$A \,=\, Q\, B + R,$$

le degré de R étant strictement inférieur à celui de B :

$$0 \,\leqslant\, \deg R \,<\, m.$$

• **Algorithme :**

► $R \longleftarrow A$.

► pour $i = n - m$, $n - m - 1$, …, 0, faire :

si $\deg R = m + i$ alors $Q_i \longleftarrow \mathsf{Tete}\,(R)/b_m$

$R \longleftarrow R - Q_i\, B$

sinon $Q_i \longleftarrow 0$

► Retourner $Q = \sum_{0 \leqslant i \leqslant n-m} Q_i$ et R.

Ici, le lecteur-étudiant est invité à déchiffrer soigneusement les instructions de cet algorithme, afin premièrement de se convaincre par la réflexion qu'il correspond bien à la situation générale exemplifiée ci-dessus, et deuxièmement, afin de reconstituer par lui-même

les arguments qui démontrent le caractère bien-fondé des calculs, et notamment, de vérifier que *l'algorithme termine en temps fini*.

Contentons-nous de détailler la démonstration d'un lemme plus simple.

Lemme 3.3. [Unicité du quotient et du reste] *Lorsque le coefficient* $b_m \in mathcalA^\times$ *du monôme de tête* $\mathbf{b_m}\,\mathbf{x^m}$ *de* $B(x)$ *est une unité, le polynôme-quotient* $Q(x)$ *et le polynôme-reste* $R(x)$ *dans la division de* $A(x)$ *par* $B(x)$ *:*

$$A \,=\, Q\,B + R,$$

sont déterminés de manière unique.

Démonstration. En effet, une autre équation :

$$A \,=\, Q'\,B + R',$$

soustraite à $A = Q\,B + R$ donne après réorganisation :

$$\big(Q' - Q\big)\,B \,=\, R - R',$$

et comme le membre de droite est de degré $\leqslant \deg B - 1$, le membre de gauche ne peut qu'être identiquement nul, d'où $Q' = Q$ puis $R' = R$. □

4. Anneaux intègres euclidiens

Pourrait-on, par une conceptualisation adéquate, capturer dans un seul filet les deux situations analogues classiques que sont :

- la division euclidienne dans $\mathbb{N}$ ou dans $\mathbb{Z}$;
- la division euclidienne dans $\mathbb{Z}[x]$ ou dans $\mathbb{Q}[x]$?

Dans les deux cas, ce qui compte, c'est l'existence d'une fonction naturelle qui mesure l'abaissement de la complexité ou de la taille des objets après une division élémentaire.

Définition 4.1. [Anneaux euclidiens] Un anneau commutatif intègre $\mathscr{A}$ muni d'une unité $1 \in \mathscr{A}$ est appelé un *anneau euclidien* s'il existe une fonction :

$$\delta\colon \quad \mathscr{A}\backslash\{0\} \,\longrightarrow\, \mathbb{N}, \qquad \delta(0) := -\infty,$$

telle que, pour tous $a, b \in \mathscr{A}$ avec $b \neq 0$, il est possible de diviser a par b avec un reste δ-inférieur au sens précis où :

$$\text{il existe } q,\, r \,\in \mathscr{A} \;\text{ avec } \boxed{\delta(r) \,<\, \delta(b)} \;\text{ satisfaisant } \boxed{a = q\,b + r}\,.$$

Bien que l'unicité de q et celle de r ne soient pas requises dans cette définition, on dit souvent que q est le *quotient* dans la division de a par b, et que r en est le *reste*.

Noter que la fonction δ est soumise à la seule condition de diriger les « abaissements de complexité » $\delta(r) < \delta(b)$.

Terminologie 4.2. On dira que δ est la *fonction euclidienne* de l'anneau euclidien $(\mathscr{A}, \delta)$.

Avec la fonction valeur absolue $\delta(a) := |a|$, il est bien connu que l'anneau des entiers naturels $\mathbb{Z}$ est un anneau euclidien, et d'ailleurs, l'unicité du quotient q et du reste r sont garanties dès lors qu'on demande que $r \geqslant 0$, ce qu'il est raisonnable de faire.

Lorsque $\mathscr{A} = K[x]$ est l'anneau des polynômes sur un corps, la fonction degré $d(a) := \deg a$, avec $\deg(0) := -\infty$, est la fonction naturelle qui munit $K[x]$ d'une structure d'anneau euclidien, l'unicité du quotient et du reste étant faciles à vérifier.

Rappelons qu'un élément $p \in \mathscr{A}$ *divise* un autre élément $q \in \mathscr{A}$ s'il existe $r \in \mathscr{A}$ satisfaisant :

$$p = r\,q.$$

Définition 4.3. [Plus grand commun diviseur] Soit $\mathscr{A}$ un anneau commutatif quelconque et soient deux éléments $a, b \in \mathscr{A}$. On dit qu'un élément $c \in \mathscr{A}$ est *un* plus grand commun diviseur entre a et b, ce qu'on note $c = \mathsf{pgcd}(a, b)$, lorsque :

- c divise a et c divise b ;
- si un élément $d \in \mathscr{A}$ divise simultanément a et b, alors en fait, d divise c

Classiquement, le fait qu'un élément $p \in \mathscr{A}$ divise un autre élément $q \in \mathscr{A}$ se note :

$$p \,|\, q.$$

Définition 4.4. [Plus petit commun multiple] Soit $\mathscr{A}$ un anneau quelconque et soient deux éléments $a, b \in \mathscr{A}$. On dit qu'un élément $e \in \mathscr{A}$ est *un* plus petit commun multiple entre a et b, ce qu'on note $e = \mathsf{ppcm}(a, b)$, lorsque :

- $a \,|\, e$ et $b \,|\, e$;
- si un élément $f \in \mathscr{A}$ est divisible simultanément par a et par b, alors en fait, $e \,|\, f$.

Certes en général, pgcd et ppcm ne sont pas, strictement parlant, uniques. Toutefois, il est aisé, sur $\mathscr{A} = \mathbb{Z}$ et sur $\mathscr{A} = \mathbb{Z}[x]$ d'assurer leur unicité (voir *infra*).

Comme on le sait, entre deux nombres quelconques $a, b \in \mathbb{Z}$, le pgcd est *unique* dès lors qu'on demande qu'il appartienne à $\mathbb{N}$. Alors le lecteur-étudiant reconstituera sans difficulté la démonstration des propriétés élémentaires du pgcd.

Lemme 4.5. *Sur l'anneau $\mathbb{Z}$ des entiers naturels, la fonction à deux arguments* $\mathsf{pgcd}(\cdot, \cdot)$ *possède les cinq propriétés suivantes :*

(i) $\mathsf{pgcd}(a, b) = |a| \Longleftrightarrow a \,|\, b$ *;*

(ii) $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(b, a)$ *;*

(iii) $\mathsf{pgcd}\big(a, \mathsf{pgcd}(b, c)\big) = \mathsf{pgcd}\big(\mathsf{pgcd}(a, b), c\big)$.

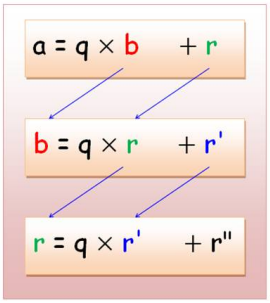
(iv) $\mathsf{pgcd}(c \cdot a,\, c \cdot b) = |c|\, \mathsf{pgcd}(a, b)$.

(v) $|a| = |b| \Longrightarrow \mathsf{pgcd}(a, c) = \mathsf{pgcd}(b, c)$. □

Notons « pour le fun » que l'associativité générale s'écrit :

$$\mathsf{pgcd}(a_1, \ldots, a_n) \;=\; \mathsf{pgcd}\big(a_1,\, \mathsf{pgcd}(a_2,\, \ldots,\, \mathsf{pgcd}(a_{n-1}, a_n) \ldots)\big).$$

Les anneaux euclidiens sont exactement ceux dans lesquels des divisions euclidiennes successives sont possibles, notamment pour trouver un pgcd entre deux éléments quelconques donnés.



En partant de deux éléments $a, b \in \mathscr{A}$ que l'on renomme $r_0, r_1 \in \mathscr{A}$ avec $\delta(r_0) \geqslant \delta(r_1)$, une première division euclidienne :

$$r_0 \;=\; q_1\, r_1 + r_2,$$

suivie de divisions successives entre les restes nouveaux $r_2, r_3, r_4, \ldots$ qui appaissent, peut être représentée synoptiquement comme suit :

$$\begin{array}{rcl}
\overset{\delta(r_0)\;\geqslant\;\delta(r_1)}{r_0} & = & q_1 r_1 \;+\; r_2 \\
\overset{\delta(r_1)\;\geqslant\;\delta(r_2)}{r_1} & = & q_2 r_2 \;+\; r_3 \\
\overset{\delta(r_2)\;\geqslant\;\delta(r_3)}{r_2} & = & q_3 r_3 \;+\; r_4 \\
\overset{\delta(r_3)\;\geqslant\;\delta(r_4)}{r_3} & = & q_4 \boxed{r_4} + \mathbf{0}
\end{array}$$

où l'on suppose ici que le procédé termine à la quatrième division, à savoir que $r_5 = 0$. Lorsque $\mathscr{A} = \mathbb{Z}$, il est bien connu alors que le pgcd est le dernier reste non nul, ici r_4, et on démontre en cours d'Algèbre que cela est encore vrai dans tout anneau euclidien $(\mathscr{A}, \delta)$.

Algorithme: Division euclidienne classique

• **Entrées :** Deux éléments $a, b \in (\mathscr{A}, \delta)$ d'un anneau commutatif intègre euclidien $\mathscr{A}$ muni d'une fonction euclidienne δ.

• **Sortie :** Un plus grand commun diviseur $h \in \mathscr{A}$ entre a et b.

► $r_0 \longleftarrow a$, $r_1 \longleftarrow b$.

► $i \longleftarrow 1$

► tant que $r_i \neq 0$ faire $r_{i+1} \longleftarrow \text{Reste}\big(r_{i-1} \text{ divisé par } r_i\big)$
$i \longleftarrow i + 1$

► Retourner r_{i-1}.

Comme cela a déjà été illustré sur l'exemple qui le précède, cet algorithme (antique) divise les restes successifs :

$$\begin{array}{rcl}
\overset{\delta(r_{i-1})\;\geqslant\;\delta(r_i)}{r_{i-1}} & = & q_i\, r_i \;+\; r_{i+1},
\end{array}$$

remplace à chaque étape les couples :

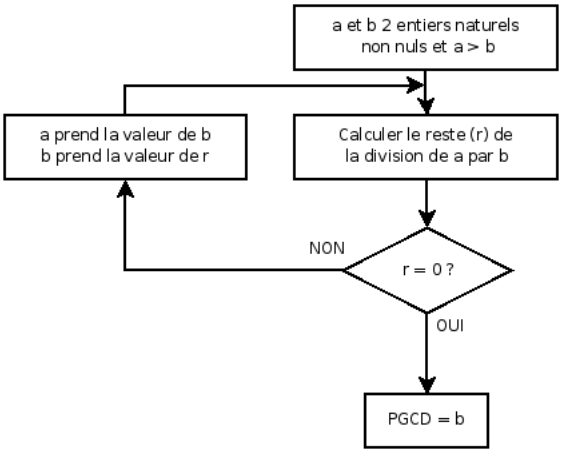
$$[r_i,\, r_{i+1}] \longleftarrow [r_{i-1},\, r_i],$$

puis recommence à diviser :

$$\begin{array}{rcl}
\overset{\delta(r_i)\;\geqslant\;\delta(r_{i+1})}{r_i} & = & q_{i+1}\, r_{i+1} \;+\; r_{i+2},
\end{array}$$

et ainsi de suite.

Sans utiliser d'indices, l'algorithme de division euclidienne classique peut aussi être représenté sous la forme d'une carte d'instructions en boucle :



Exemple 4.6. Il est avisé de représenter synoptiquement la recherche, déjà entamée *supra*, du pgcd entre 126 et 35 :

$$\begin{aligned} 126 &\overset{126 \;\geqslant\; 35}{=} 3\cdot 35 + 21 \\ 35 &\overset{35 \;\geqslant\; 21}{=} 1\cdot 21 + 14 \\ 21 &\overset{21 \;\geqslant\; 14}{=} 1\cdot 14 + 7 \\ 14 &\overset{14 \;\geqslant\; 7}{=} 2\cdot \boxed{7} + 0, \end{aligned}$$

et ici, puisque le cinquième reste $r_5 = 0$ est nul, l'avant-dernier reste $r_4 = 7$ est un (le) pgcd recherché.

Exemple 4.7. De manière alternative, on peut représenter sous forme d'un tableau le calcul qui montre que 315 et 307 sont premiers entre eux.

	Dividende	Diviseur	Reste
315 =1 x 307 + 8	315	307	8
307 = 8 x 38 + 3	307	8	3
8 = 2 x 3 + 2	8	3	2
3 = 2 x 1 + 1	3	2	1
2 = 2 x 1 + 0	2	1	0

5. Croissance des expressions intermédiaires et normalisations

Les calculs avec des polynômes, des fractions rationnelles, ou des matrices à coefficients entiers souffrent souvent d'une « maladie » propre au calcul numérique ou symbolique : *la croissance parfois débridée des expressions.*

Exemple 5.1. Voici le déroulement du calcul du plus grand commun diviseur entre les deux polynômes à coefficients entiers :

$$\begin{aligned} A &= \mathbf{7}\,\mathbf{x^5} - 22\,x^4 + 55\,x^3 + 94\,x^2 - 87\,x + 56 \\ &=: R_0, \\ B &= \mathbf{62}\,\mathbf{x^4} - 97\,x^3 + 73\,x^2 + 4\,x + 83 \\ &=: R_1, \end{aligned}$$

au moyen de l'algorithme d'Euclide ; à cause notamment du fait que les deux coefficients de tête $\mathbf{7}$ et $\mathbf{62}$ de A et de B ne sont pas des unités, les polynômes-restes dans les divisions successives :

$$\begin{aligned} R_2 &:= \text{reste dans la division de } R_0 \text{ par } R_1, \\ R_3 &:= \text{reste dans la division de } R_1 \text{ par } R_2, \\ R_4 &:= \text{reste dans la division de } R_2 \text{ par } R_3, \\ R_5 &:= \text{reste dans la division de } R_3 \text{ par } R_4, \end{aligned}$$

possèdent des coefficients rationnels qui « explosent » de manière assez surprenante :

$$\begin{aligned} R_2 &= \frac{113293}{3844}\,x^3 + \frac{409605}{3844}\,x^2 - \frac{183855}{1922}\,x + \frac{272119}{3844}, \\ R_3 &= \frac{18423282923092}{12835303849}\,x^2 - \frac{15239170790368}{12835303849}\,x + \frac{10966361258256}{12835303849}, \\ R_4 &= -\frac{216132274653792395448637}{44148979404824831944178}\,x - \frac{631179956389122192280133}{88297958809649663888356}, \\ R_5 &= \frac{20556791167692068695002336923491296504125}{3639427682941980248860941972667354081}. \end{aligned}$$

Afin de remédier — au moins en partie — à ce phénomène, il est avisé de *normaliser systématiquement* les polynômes intermédiaires de manière à ce que le coefficient de leur terme de tête soit toujours égal à 1.

Terminologie 5.2. Étant donné un polynôme de degré $k \geqslant 0$:

$$P(x) = \mathbf{c_k}\,\mathbf{x^k} + c_{k-1}\,x^{k-1} + \cdots + +c_0 \qquad (c_k \neq 0),$$

on appelle *coefficient de tête* le nombre :

$$\mathbf{c_k} \in \mathscr{A},$$

et on dit que P *unitaire* lorsque :

$$\mathbf{c_k} = 1.$$

Par exemple, dans l'anneau $\mathscr{A} = \mathbb{Q}[x]$ des polynômes à coefficients dans le *corps* des nombres rationnels, on peut toujours *diviser* $P(x)$ par son coefficient de tête de manière à le rendre *unitaire :*

$$\frac{1}{\mathbf{c_k}}\,P(x) = \mathbf{x^k} + \frac{c_{k-1}}{c_k}\,x^{k-1} + \cdots + \frac{c_0}{c_k}.$$

Une expérience renouvelée des calculs à la main ou sur ordinateur a montré que dans l'algorithme d'Euclide, il est avisé de *rendre unitaires tous les restes intermédiaires* afin de rabaisser la complexité des coefficients rationnels des polynômes. Au final, après exécution de toutes les divisions euclidiennes requises, le polynôme pgcd entre deux polynômes donnés $A, B \in \mathbb{Q}[x]$:

$$\mathsf{pgcd}(A, B) \in \mathbb{Q}[x],$$

sera connu à un facteur rationnel non nul près.

Bien entendu, ce qui est vrai ici pour $\mathbb{Q}[x]$ est vrai aussi pour tout anneau de polynômes $K[x]$ à coefficients dans un corps commutatif K.

Mais comment s'y prendre si l'on désire travailler, plus généralement, avec l'anneau des polynômes à coefficients dans un anneau euclidien $\mathscr{A}$ qui n'est pas forcément un corps ?

Il suffit — certes un peu artificiellement — de demander l'existence de formes normales au sens précis qui suit.

Définition 5.3. Un anneau euclidien est dit *normal* si tout élément $a \in \mathscr{A}$ possède une forme normale unique :

$$\mathsf{Normal}(a) \in \mathscr{A}$$

qui diffère de a simplement par une unité :

$$a = u \cdot \mathsf{Normal}(a) \qquad (u \in \mathscr{A}^\times),$$

la forme normale d'un produit quelconque entre deux éléments $a, b \in \mathscr{A}$ étant égale au produit des formes normales :

$$\mathsf{Normal}(a\,b) = \mathsf{Normal}(a)\,\mathsf{Normal}(b),$$

deux éléments $a \in \mathscr{A}$ et $a' \in \mathscr{A}$ ayant la même forme normale :

$$\mathsf{Normal}(a) = \mathsf{Normal}(a')$$

lorsque, et seulement lorsque, ils diffèrent d'une unité :

$$a' = u\,a \qquad (u \in \mathscr{A}^\times).$$

Il est avisé d'introduire une notation pour l'unité dont un élément $a \in \mathscr{A}$ et sa forme normale diffèrent :

$$\boxed{\mathsf{Unite}(a) := \frac{a}{\mathsf{Normal}(a)}}.$$

Dans un anneau euclidien normal, pgcd et ppcm entre deux éléments quelconques sont alors définis de manière unique, simplement en prenant les formes normales.

Exercice 2. Justifer l'affirmation qui précède.

Exercice 3. **(a)** Sur $\mathscr{A} = \mathbb{Z}$, déterminer la forme normale naturelle d'un entier.

(b) Faire de même sur $\mathscr{A} = K[x]$, où K est un corps.

(c) En utilisant la normalisation de **(a)**, traiter l'algorithme d'Euclide qui permet de calculer le pgcd entre deux entiers relatifs quelconques $a, b \in \mathbb{Z}$.

6. Algorithme d'Euclide étendu

Soit $(\mathscr{A}, \delta)$ un anneau commutatif unitaire euclidien normal. L'idée pour raffiner l'algorithme d'Euclide, simple et déjà comprise plus haut, consiste, lorsqu'on divise itérativement, à normaliser les restes à chaque étape. En tout cas, sans remplacer les restes intermédiaires par leurs formes normales, en partant de deux éléments $a, b \in \mathscr{A}$ avec $\delta(b) \leqslant \delta(a)$ que l'on renomme :

$$r_0 := a \qquad \text{et} \qquad r_1 := b,$$

rappelons que l'algorithme de divisions successives jusqu'à épuisement se représente comme suit :

$$\begin{aligned}
r_0 &= q_1\, r_1 + r_2,\\
r_1 &= q_2\, r_2 + r_3,\\
&\ddots\quad \ddots\quad \ddots\\
r_{i-1} &= q_i\, r_i + r_{i+1},\\
&\ddots\quad \ddots\quad \ddots\\
r_{\ell-2} &= q_{\ell-1}\, r_{\ell-1} + \boxed{r_\ell},\\
r_{\ell-1} &= q_\ell\, \boxed{r_\ell} + \mathbf{0},
\end{aligned}$$

le dernier reste non nul valant :

$$r_\ell \;=\; \mathsf{pgcd}(r_0, r_1) \;=\; \mathsf{pgcd}(a, b).$$

Maintenant, si l'on souhaite faire voir que les restes intermédiaires doivent être normalisés, on les représentera sous la forme :

$$\rho_i\, r_i \qquad \text{avec} \qquad \begin{aligned} \rho_i &= \mathsf{Unite}\big(\rho_i\, r_i\big),\\ r_i &= \mathsf{Normal}(\rho_i\, r_i), \end{aligned}$$

et en supposant pour simplifier que l'on a déjà normalisé au départ :

$$\begin{aligned}
r_0 &:= \mathsf{Normal}(a), \qquad & \rho_0 &:= \mathsf{Unite}(a), \qquad & a &= \rho_0\, r_0,\\
r_1 &:= \mathsf{Normal}(b), \qquad & \rho_1 &:= \mathsf{Unite}(b), \qquad & b &= \rho_1\, r_1,
\end{aligned}$$

de telle sorte les nouveaux restes intermédiaires avec spécification de normalisation s'écriront :

$$\rho_2\, r_2,\;\; \rho_3\, r_3,\;\; \ldots\ldots,\;\; \rho_\ell\, r_\ell,$$

on obtiendra la représentation synoptique :

$$\begin{aligned}
r_0 &= q_1\, r_1 + \rho_2\, r_2,\\
r_1 &= q_2\, r_2 + \rho_3\, r_3,\\
&\ddots\quad \ddots\quad \ddots\\
r_{i-1} &= q_i\, r_i + \rho_{i+1}\, r_{i+1},\\
&\ddots\quad \ddots\quad \ddots\\
r_{\ell-2} &= q_{\ell-1}\, r_{\ell-1} + \boxed{\rho_\ell\, r_\ell},\\
r_{\ell-1} &= q_\ell\, \boxed{r_\ell} + \mathbf{0}.
\end{aligned}$$

De plus, il s'avère dans certaines applications arithmétiques du calcul de pgcd que *tous* les résultats intermédiaires possèdent une utilité. Si donc l'on part de deux éléments quelconques $a, b \in \mathscr{A}$ d'un anneau euclidien normal $\mathscr{A}$, une organisation systématique (*voir* ce qui va suivre) des calculs donnera au final l'*identité de Bézout :*

$$s_\ell\, a + t_\ell\, b = \mathsf{pgcd}(a, b),$$

mais à chaque étape intermédiaire, on devra aussi écrire :

$$s_i\, a + t_i\, b \;=\; r_i \qquad (0 \leqslant i \leqslant \ell). \tag{$*$}$$

En fait, il est aisé d'expliquer comment construire par récurrence de tels éléments s_i, t_i. Pour $i = 0$ et pour $i = 1$, on a tout d'abord :

$$\frac{1}{\rho_0} \cdot a + \mathbf{0} \cdot b \;=\; r_0 \;=:\; s_0\, a + t_0\, b,$$
$$\mathbf{0} \cdot a + \frac{1}{\rho_1} \cdot b \;=\; r_1 \;=:\; s_1\, a + t_1\, b,$$

ce qui donne sans difficulté des couples (s_0, t_0) et (s_1, t_1) qui conviennent.

En raisonnant par récurrence, supposons pour un certain entier i avec $1 \leqslant i \leqslant \ell - 1$, on ait déjà obtenu aux deux niveaux i et $i - 1$:

$$s_{i-1}\, a + t_{i-1}\, b \;=\; r_{i-1},$$
$$s_i\, a \;+\; t_i\, b \;=\; r_i.$$

Alors en partant de l'identité de division euclidienne dans laquelle naît le $(i+1)$-ème reste (normalisé) :

$$r_{i-1} \;=\; q_i\, r_i + \rho_{i+1}\, r_{i+1},$$

en réécrivant cette identité et en y insérant les deux identités admises par récurrence :

$$\begin{aligned} \rho_{i+1}\, r_{i+1} \;&=\; r_{i-1} - q_i\, r_i \\ &=\; s_{i-1}\, a + t_{i-1}\, b - q_i\big(s_i\, a + t_i\, b\big) \\ &=\; \big(s_{i-1} - q_i\, s_i\big)\, a + \big(t_{i-1} - q_i\, t_i\big)\, b, \end{aligned}$$

d'où après division par l'unité ρ_{i+1} :

$$\begin{aligned} r_{i+1} \;&=\; \left(\frac{s_{i-1} - q_i\, s_i}{\rho_{i+1}}\right) a + \left(\frac{t_{i-1} - q_i\, t_i}{\rho_{i+1}}\right) b \\ &=:\; s_{i+1}\, a + t_{i+1}\, b, \end{aligned}$$

ce qui donne les relations de récurrence :

$$\boxed{s_{i+1} \;:=\; \frac{s_{i-1} - q_i\, s_i}{\rho_{i+1}} \qquad \text{et} \qquad t_{i+1} \;:=\; \frac{t_{i-1} - t_i\, s_i}{\rho_{i+1}}}.$$

Nous pouvons maintenant formuler l'énoncé des instructions avant de démontrer qu'elles sont correctes.

Algorithme: Division euclidienne étendue avec mémorisations

• **Entrées :** Deux éléments $a, b \in \mathscr{A}$ d'un anneau euclidien normal.

• **Sorties :** Un entier d'arrêt $\ell \in \mathbb{N}$, une collection d'éléments $\rho_i, r_i, s_i, t_i \in \mathscr{A}$ pour $0 \leqslant i \leqslant \ell + 1$, et des quotients $q_i \in \mathscr{A}$ pour $0 \leqslant i \leqslant \ell$, calculés comme suit.

• **Algorithme :**

► $\rho_0 \longleftarrow \mathsf{Unite}(a)$, $\quad r_0 \longleftarrow \mathsf{Normal}(a)$, $\quad s_0 \longleftarrow 1/\rho_0$, $\quad t_0 \longleftarrow 0$.

► $\rho_1 \longleftarrow \mathsf{Unite}(b)$, $\quad r_1 \longleftarrow \mathsf{Normal}(b)$, $\quad s_1 \longleftarrow 0$, $\quad t_1 \longleftarrow 1/\rho_1$.

► $i \longleftarrow 1$

tant que $r_i \neq 0$ faire

$q_i \longleftarrow$ quotient$\big(r_{i-1}$ divisé par $r_i\big)$

$\rho_{i+1} \longleftarrow \mathsf{Unite}\big(\mathsf{Reste}(r_{i-1}$ divisé par $r_i)\big)$

$r_{i+1} \longleftarrow \mathsf{Normal}\big(\mathsf{Reste}(r_{i-1}$ divisé par $r_i)\big)$

$s_{i+1} \longleftarrow \big(s_{i-1} - q_i\, s_i\big)\big/\rho_{i+1}$
$t_{i+1} \longleftarrow \big(t_{i-1} - q_i\, t_i\big)\big/\rho_{i+1}$
$i \longleftarrow i+1$

► $\ell \longleftarrow i-1$

► Retourner ℓ, ρ_i, r_i, s_i, t_i pour $0 \leqslant i \leqslant \ell+1$, et q_i pour $1 \leqslant i \leqslant \ell$

Démonstration. On commence donc par normaliser a et b en introduisant :

$$r_0 \;:=\; \frac{a}{\rho_0} \;=\; \mathsf{Normal}(a) \;=\; \mathsf{Normal}(r_0),$$
$$r_1 \;:=\; \frac{b}{\rho_1} \;=\; \mathsf{Normal}(b) \;=\; \mathsf{Normal}(r_1).$$

Comme cela vient d'être implicitement décrit dans la formulation de cet algorithme d'Euclide étendu, les calculs fournissent les relations suivantes entre les quantités r_i, s_i, t_i :

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl}
\rho_2\, r_2 &=& r_0 - q_1\, r_1, & \rho_2\, s_2 &=& s_0 - q_1\, s_1, & \rho_2\, t_2 &=& t_0 - q_1\, t_1, \\
\vdots &=& \vdots & \vdots &=& \vdots & \vdots &=& \vdots \\
\rho_{i+1}\, r_{i+1} &=& r_{i-1} - q_i\, r_i, & \rho_{i+1}\, s_{i+1} &=& s_{i-1} - q_i\, s_i, & \rho_{i+1}\, t_{i+1} &=& t_{i-1} - q_i\, t_i, \\
\vdots &=& \vdots & \vdots &=& \vdots & \vdots &=& \vdots \\
0 &=& r_{\ell-1} - q_\ell\, r_\ell, & \rho_{\ell+1}\, s_{\ell+1} &=& s_{\ell-1} - q_\ell\, s_\ell, & \rho_{\ell+1}\, t_{\ell+1} &=& t_{\ell-1} - q_\ell\, t_\ell,
\end{array}$$

la première colonne ayant déjà été vue, tandis que la seconde et la troisième, en partant de :

$$\begin{array}{lll@{\qquad}lll}
s_0 &:=& \frac{1}{\rho_0}, & t_0 &:=& 0, \\
s_1 &:=& 0, & t_1 &:=& \frac{1}{\rho_1},
\end{array}$$

définissent par induction les quantités :

$$s_2, \ldots, s_{\ell+1} \qquad \text{et} \qquad t_2, \ldots, t_{\ell+1},$$

dont la nature s'éclaircira dans un instant, *cf.* l'équation $(*)$ ci-dessus.

Sachant que les deux multiplicateurs de Bézout s_i et t_i se transforment simultanément à chaque étape de l'algorithme, il est naturel de raisonner en termes de matrices 2×2, et plus précisément, il est naturel d'introduire la matrice :

$$R_0 \;:=\; \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \;=\; \begin{pmatrix} \frac{1}{\rho_0} & 0 \\ 0 & \frac{1}{\rho_1} \end{pmatrix},$$

accompagnée des ℓ matrices :

$$Q_i \;:=\; \begin{pmatrix} 0 & 1 \\ \frac{1}{\rho_{i+1}} & -\frac{q_i}{\rho_{i+1}} \end{pmatrix} \qquad (1 \leqslant i \leqslant \ell),$$

et enfin, d'introduire aussi les ℓ produits de matrices :

$$R_i \;:=\; Q_i \cdots Q_1\, R_0 \qquad (1 \leqslant i \leqslant \ell).$$

Lemme $*$. *Pour tout entier intermédiaire i avec $0 \leqslant i \leqslant \ell$, on a :*

$$R_i \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix},$$

et de plus, ces matrices R_i valent :

$$R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}.$$

avec la convention que $\rho_{\ell+1} = 1$ et que $r_{\ell+1} = 0$.

Démonstration. En effet, pour $i = 0$, on a tout d'abord bien :

$$\begin{aligned} R_0 \cdot \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{\rho_0} & 0 \\ 0 & \frac{1}{\rho_1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \frac{a}{\rho_0} \\ \frac{b}{\rho_1} \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}. \end{aligned}$$

Après cela, en supposant par récurrence que l'on a déjà au niveau i :

$$Q_i \cdots Q_1 R_0 \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix},$$

il suffit de multiplier cette équation par la matrice Q_{i+1} pour atteindre le niveau $i+1$:

$$\begin{aligned} Q_{i+1} Q_i \cdots Q_1 R_0 \cdot \begin{pmatrix} a \\ b \end{pmatrix} &= Q_{i+1} \cdot \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ \frac{1}{\rho_{i+2}} & -\frac{q_{i+1}}{\rho_{i+2}} \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \\ &= \begin{pmatrix} r_{i+1} \\ \frac{r_i}{\rho_{i+2}} - \frac{q_{i+1} r_{i+1}}{\rho_{i+2}} \end{pmatrix} \\ &= \begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix}. \end{aligned}$$

Ensuite, si, à un certain niveau i avec $0 \leqslant i \leqslant \ell$, la matrice R_i possède bien l'expression annoncée (ce qui est d'emblée le cas pour $i = 0$), alors au niveau $i+1$, puisque :

$$R_{i+1} = Q_{i+1} R_i,$$

on déduit l'expression :

$$\begin{aligned} Q_{i+1} \cdot \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ \frac{1}{\rho_{i+2}} & -\frac{q_{i+1}}{\rho_{i+2}} \end{pmatrix} \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} \\ &= \begin{pmatrix} s_{i+1} & t_{i+1} \\ \frac{s_i - q_{i+1} s_{i+1}}{\rho_{i+2}} & \frac{t_i - q_{i+1} t_{i+1}}{\rho_{i+2}} \end{pmatrix} \\ &= \begin{pmatrix} s_{i+1} & t_{i+1} \\ s_{i+2} & t_{i+2} \end{pmatrix}, \end{aligned}$$

ce qui termine la démonstration. □

L'égalité matricielle de ce lemme s'écrit donc :

$$\begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix},$$

et elle donne, pour tout $0 \leqslant i \leqslant \ell + 1$, les *identités de Bézout intermédiaires :*

$$\boxed{s_i\, a + t_i\, b \;=\; r_i}.$$

Au niveau $i = \ell + 1$, puisque le dernier reste $r_{\ell+1} = 0$ est nul, on a donc :

$$s_{\ell+1}\, a + t_{\ell+1}\, b \;=\; 0,$$

et au niveau $i = \ell$ juste avant, on a l'*identité de Bézout :*

$$\boxed{s_\ell\, a + t_\ell\, b \;=\; r_\ell}.$$

puis que nous pouvons maintenant démontrer effectivement que :

$$r_\ell \;=\; \mathsf{pgcd}(a, b).$$

Lemme $*$**.** *Avec les mêmes notations, toujours pour* $i = 0, 1, \ldots, \ell$*, les cinq propriétés suivantes sont satifaites :*

(i) $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(r_i, r_{i+1}) = r_\ell$;

(ii) $s_i\, t_{i+1} - t_i\, s_{i+1} = \frac{(-1)^i}{\rho_0 \cdots \rho_{i+1}}$*, et* $\mathsf{pgcd}(s_i, t_i) = 1$;

(iii) $\mathsf{pgcd}(r_i, t_i) = \mathsf{pgcd}(a, t_i)$;

(iv)

$$\begin{aligned} a \;&=\; (-1)^i\, \rho_0 \cdots \rho_{i+1} \big(t_{i+1}\, r_i - t_i\, r_{i+1}\big), \\ b \;&=\; (-1)^{i+1}\, \rho_0 \cdots \rho_{i+1} \big(s_{i+1}\, r_i - s_i\, r_{i+1}\big). \end{aligned}$$

Démonstration. Pour **(i)**, soit $i \in \{0, \ldots, \ell\}$. Grâce au lemme qui précède vu au niveau ℓ, on a :

$$\begin{aligned} \begin{pmatrix} r_\ell \\ 0 \end{pmatrix} \;=\; R_\ell \begin{pmatrix} a \\ b \end{pmatrix} \;&=\; Q_\ell \cdots Q_{i+1} R_i \begin{pmatrix} a \\ b \end{pmatrix} \\ &=\; Q_\ell \cdots Q_{i+1} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}. \end{aligned}$$

Cette identité montre que r_ℓ est une combinaison linéaire de r_i et de r_{i+1}, donc *le* pgcd normalisé entre r_i et r_{i+1} divise r_ℓ.

D'un autre côté, puisque le déterminant :

$$\det Q_i \;=\; -\tfrac{1}{\rho_{i+1}}$$

est une unité dans $\mathscr{A}$, la matrice Q_i est inversible, d'inverse :

$$Q_i^{-1} \;=\; \begin{pmatrix} q_i & \rho_{i+1} \\ 1 & 0 \end{pmatrix}$$

ce qui nous permet d'inverser aisément l'identité que nous venons d'obtenir :

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \;=\; Q_{i+1}^{-1} \cdots Q_\ell^{-1} \begin{pmatrix} r_\ell \\ 0 \end{pmatrix}.$$

Ceci montre que r_i et r_{i+1} sont tous les deux divisibles par r_ℓ.

Enfin, puisque r_ℓ est normal, et puisque le pgcd est défini de manière unique en passant à la forme normale, il en découle que :

$$r_\ell \;=\; \mathsf{pgcd}(r_i,\, r_{i+1}),$$

ce qui, au niveau $i = 0$, donne :

$$\mathsf{pgcd}(a, b) \;=\; \mathsf{pgcd}(r_0, r_1) = r_\ell.$$

Ensuite, **(ii)** se vérifie en calculant des produits de déterminants :

$$\begin{aligned} s_i\, t_{i+1} - t_i\, s_{i+1} \;&=\; \det \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} \;=\; \det R_i \;=\; \det Q_i \cdots \det Q_1 \det \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \\ &=\; \frac{(-1)^i}{\rho_{i+1} \cdots \rho_2 \rho_1 \rho_0}, \end{aligned}$$

ce qui implique (exercice mental) que :

$$\boxed{\mathsf{pgcd}(s_i, t_i) \;=\; 1}.$$

Maintenant pour **(iii)**, observons que les deux pgcd incorporent t_i. Pour montrer qu'il sont égaux, il suffit donc (exercice mental) de faire voir que pour tout diviseur d de t_i :

$$d \,|\, a \iff d \,|\, r_i.$$

Soit donc d un diviseur quelconque de t_i.

Si $d \,|\, a$, alors aussi d divise $s_i\, a + t_i\, b = r_i$.

Inversement, si d divise r_i, alors aussi d divise $r_i - t_i\, b = s_i a$. Mais comme $\mathsf{pgcd}(s_i, t_i) = 1$, tout diviseur d de t_i est premier avec s_i, et donc si d divise $s_i\, a$, c'est que d doit diviser a.

Pour **(iv)**, puisque qu'il découle de **(ii)** (exercice visuel) que la matrice R_i est inversible d'inverse :

$$R_i^{-1} \;=\; (-1)^i\, \rho_0 \cdots \rho_{i+1} \begin{pmatrix} t_{i+1} & -\,t_i \\ -\,s_{i+1} & s_i \end{pmatrix}$$

on peut récrire l'identité du lemme qui précède sous la forme :

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} \;&=\; R_i^{-1} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \\ &=\; (-1)^i\, \rho_0 \cdots \rho_{i+1} \begin{pmatrix} t_{i+1} & -\,t_i \\ -\,s_{i+1} & s_i \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \\ &=\; (-1)^i\, \rho_0 \cdots \rho_{i+1} \begin{pmatrix} t_{i+1}\, r_i - t_i\, r_{i+1} \\ -\,s_{i+1}\, r_{i+1} + s_i\, r_{i+1} \end{pmatrix} \end{aligned}$$

ce qui conclut la démonstration □

L'explication démonstrative de l'Algorithme de division euclidienne étendue est achevée. □