From Euclide to Padé

COURTOIS Sandrine
sandrine.courtois@voila.fr

March 14, 2007

Contents

Chapter 1

Introduction

1.1 Présentation du sujet

L'article *From Euclide to Padé* examine les relations existant entre les algorithmes apparemment étrangers les uns aux autres.
Ces algorithmes concernent aussi bien le calcul exact que la théorie de l'approximation.
Il sera rappelé comment une écriture efficace de l'algorithme d'Euclide conduit non seulement aux coefficients de **Bezout**, de son prénom **Etienne**, mais aussi au développement d'un réel en *fraction continue*. Appliquée aux fonctions, cette façon de faire conduit à la fois à la décomposition d'une *fraction rationnelle* en *éléments simples* et aux approximants de `Padé` pour une fonction *holomorphe*. Cet article examine aussi les questions de programmation et de visualisation liées à ces algorithmes. Ces notions seront définies tout au long de ce mémoire.

En résumé, l'objectif de ce TER est d'élargir le champ des applications de l'algorithme d'Euclide, dans un langage étudié afin d'être compréhensible par un large échantillon de personnes non forcément spécialisées en Algèbre.

1.2 Biographie d'Euclide

Un homme connu sans vie

Euclide est né à Alexandrie, Egypte, en 365 avant J.C, et meurt vers l'an 300, toujours avant J.C. C'est ici que sa biographie se termine, le reste de sa vie est un mystère, nous laissant donc imaginer ce qu'a pu faire cet homme pendant cette quarantaine d'années. Peut-être dormait-il, ou sortait-il se promener, voire même voyager, mais sûrement il passait beaucoup de temps à lire et écrire. En effet, Euclide laisse derrière lui une collection de livres précieux, dont le plus connu est ***Eléments***, portant sur ce que nous connaissons aujourd'hui comme la géométrie euclidienne.

Contrairement à d'autres auteurs, il serait impossible d'en déduire au moins certains fragments de sa vie. Jusqu'à maintenant, nous avons pu reposer toutes nos notions et théorèmes sur ses déductions, faites à partir des quelques définitions et propriétés admises sans démonstrations. Nous avons en fait reposé tout notre raisonnement géométrique sur un homme qui ne connaissait rien aux équations ou coefficients, et sur ses déductions acceptées sans questions.

Heureusement, les raisonnements de ce mathématicien ne sont pas du tout faux, mais au contraire, ils sont très logiquement basés sur des quantités geométriques. Bien sûr, cela n'est pas l'avis de tout mathématicien car il existe maintenant la géométrie non-Euclidienne, qui a pour but de réfuter tout argument utilisé par Euclide dans ses oeuvres.
Une chose est sûre, c'est qu'Euclide reçut beaucoup d'aide pour réaliser "son" oeuvre. C'est à dire qu"**Elements**" est un assemblage de différentes demonstrations des contemporains d'Euclide, que ce dernier a altérées et a réarrangées pour pouvoir les appliquer à sa manière personnelle. Ainsi, ce n'était sûrement pas Euclide qui a écrit ses livres car, comme l'était une méthode plus ou moins courante de ce temps, nous pourrions imaginer qu'Euclide faisait écrire ses livres par ses élèves.
Depuis sa première apparition, l'oeuvre d'Euclide fut utilisée sans modification en tant que base de toute éducation de la géométrie, ce qui dura à peu près 2000 ans. Ce n'est alors, pas avant le 19ème siècle que les méthodes de géométrie non Euclidenne commencèrent à apparaitre vu qu'elles nécessitent l'utilisation de fonctions circulaires et hyperboliques, alors que les grecs ne disposaient que de l'algègre babylonien (d'où provient l'apparition de la méthode axiomatique). Par conséquent, ceci créa un mouvement chaotique dans l'éducation. Encore aujourd'hui, ces 2 méthodes sont en opposition.

1.3 Chronologie des Mathématiques avant J.C.

Préhistoire -20000	Des entailles dans le bois représentent les nombres
Sumer -3500	⋆ Numérotation de position en base 60 ⋆ Les nombres sont basés sur la valeur des chiffres selon leur position ⋆ Ils inventent un zéro de position, mais ne le considèrent pas comme un chiffre ⋆ Il n'y a pas de zéro: c'est plutôt l'espace vide aumilieu d'un nombre (pas possible aux extrémités). On différencie 102 et 12 mais pas 12 et 120
Mésopotamie $-3000/-2000$	⋆ Calendriers ⋆ Mesures topologiques ⋆ Solutions de certaines équations du 2d degré ⋆ Utilisation des nombres négatifs
Babylone $-1900/-1600$	⋆ Invention probable du boulier ⋆ Ils donnent la valeur $\sqrt{2}$, sans révéler comment ils ont fait ⋆ Triplets de Pythagore, 100 ans avant Pythagore: $a^2+b^2=c^2$ qui donne 15 solutions dont (3,4,5);(65,72,97);(12709,13500,18541) (triplets ordonnés par angle décroissant de 45° à 31°)
Egyptiens $-2000/-1700$	⋆ Ils utilisent la géométrie pour résoudre des problèmes pratiques ⋆ A'hmosé décrit des méthodes pour résoudre des problèmes mathématiques: un des plus anciens documents connu.
Grecs Antiquité	⋆ Ils introduisent les outils que nous connaissons aujourd'hui: déductions, preuves, théorèmes, abstractions
Thalès de Milet $-625/-547$ (78 ans)	⋆ Utilise pour la première fois les démonstrations déductives ⋆ Ramène des connaissances de Babylone et d'Egypte ⋆ Théorème de Thalès (AB/AC=A'B'/A'C') ⋆ Célèbre pour avoir prévu une éclipse (-585) ⋆ Observe l'attraction du fer par certains minerais de fer
Pythagore $-570/-490$ ans (80 ans)	⋆ Il fonde une confrérie basée sur les mathématiques: association ⋆ scientifique, philosophique, politique et religieuse ⋆ Théorème de Pythagore: ($h^2=a^2+b^2$), connu de Babylone ⋆ On ne sait pas si Pythagore a démontré lui-même ce théorème ⋆ Mysticisme des nombres: "Tout est nombre". Les nombres sont le principe des choses

	⋆ Les nombres sont figurés par des assemblages de points: carrés, triangles, pentagones... ⋆ Crise suite à la découverte de l'incommensurabilité de la diagonale du carré ($\sqrt{2}$)
Zénon d'Elée -460	⋆ Invente des paradoxes tels que celui d'Achille et la tortue: la tortue a un peu d'avance. Au moment où Achille atteindra ce point, la tortue aura avancé. Au moment où Achille atteindra ce nouveau point, la tortue aura avancé... Achille ne peut jamais rattraper la tortue
Hippasus -441	⋆ Montre que $\sqrt{2}$ est irrationnel ⋆ A cette époque, beaucoup de mathématiciens n'acceptent pas l'idée qu'un nombre puisse être irrationnel
Platon -380	⋆ Fonde l'Académie à Athènes: "Personne, ignorant la géométrie, ne doit entrer ici". ⋆ Compose au moins 28 dialogues: devoir, mensonge, nature de l'homme ⋆ Mythe de la caverne: du monde sensible vers le monde intelligible de la vérité
Eudoxus -371	⋆ Développe la théorie des "proportions égales", le point de départ de la théorie des nombres réels. Cette théorie ne fut pas bien comprise du fait du rejet des nombres irrationnels. Elle fut ignorée durant 2000 ans jusqu'à ce que Dedekind et Cantor créent le système des nombres réels. ⋆ Euxodus développe la méthode exhaustive, une amorce de l'analyse
Menaechmus -350	⋆ Décrit les sections coniques: cercles, ellipses, paraboles, hyperboles
Euclide -300 environ	⋆ L'un des premiers membres de "l'Université d'Alexandrie" ⋆ Publie ***Les Eléments*** ⋆ "Eléments de géométrie": vaste synthèse de la géométrie classique grecque qui restera une oeuvre de référence pendant 2000 ans ⋆ Son fameux $5^{\text{ème}}$ postulat: deux parallèles ne se rencontrent jamais ⋆ Etudie les sections coniques, fonde l'école de maths d'Alexandrie ⋆ Si un nombre premier divise un produit, il divise l'un des facteurs ⋆ Unicité de la factorisation des nombres: théorème fondamental de l'arithmétique. Il y a une infinité des nombres premiers ⋆ Méthode de calcul du Plus Grand Commun Diviseur
Eratosthène $-284/-192$	⋆ Calcule la longueur du méridien terrestre avec une précision stupéfiante

Chapter 2

Euclide classique

2.1 Algorithme d'Euclide

Définition 2.1.1 (PGCD) *Pour $a \in \mathbb{Z}, b \in \mathbb{Z}$, on note:*
$\delta(a,b) \ = \{d \in \mathbb{Z}; d|a \text{ et } d|b\}$ *l'ensemble de leurs diviseurs communs.*
Le plus grand élément de $\delta(a,b)$ (pour l'ordre usuel) s'appelle le plus grand commun diviseur *de a et b. On le note $a \wedge b$ ou (a,b), ou encore $PGDC(a,b)$.*

Définition 2.1.2 (PPCM)

Exemple:

Considérons la fraction rationnelle: $\frac{28}{21}$
Décomposons chaque terme en produit de nombres premiers: $28 = 7 \times 2 \times 2$ et $21 = 7 \times 3$ Ainsi, le plus grand nombre qui divise 28 et 21 est 7.
Donc $28 \wedge 21 = 7$

Dans le cas précédent, déterminer le PGCD de 2 nombres relativement petits est aisé. Mais quand leur décomposition en produit de nombres premiers se compte en vingtaines, le travail devient laborieux. Pour lever ce problème, Euclide a trouvé un algorithme qui limite les calculs et les feuilles de papier utilisées: c'est **l'algorithme des divisions successives** que nous décrirons plus bas. Auparavant, introduisons d'autres notions nécessaires à la compréhension du lecteur.

Définition 2.1.3 (Nombres premiers entre eux) *On dit que a et b sont* premiers entre eux *si $a \wedge b = 1$.*

Remarque:

L'existence du PGCD vient du fait que $\delta(a,b)$ est une partie non vide de $\mathbb{Z}$ ($1 \in \delta(a,b)$ car 1 divise tout entier de $\mathbb{Z}$, donc en particulier a et b), majorée par $|a|$.
On constate également que $a \wedge b \in \mathbb{N}$ car $d \in \delta(a,b) \Longleftrightarrow -d \in \delta(a,b)$ ▲

Théorème 2.1.1 (de Bezout: 1730-1783) *Pour que a et $b \in \mathbb{Z}$ soient* premiers entre eux*, il faut et il suffit qu'il existe $(u,v) \in \mathbb{Z}^2$ tels que:*

$$au + bv = 1$$

Plus généralement, $\exists (u,v) \in \mathbb{Z}^2$ tels que: $au + bv = (a \wedge b)$.

N.B: Ecrire une relation de Bezout entre 2 nombres revient à déterminer u et v qui vérifient l'égalité ci-dessus.

Démonstration:

$\Longleftarrow$:

L'existence d'une relation de Bezout est une condition suffisante pour que $a \wedge b = 1$.
En effet, si $au + bv = 1$, si $d \in \delta(a,b)$, alors $d|au$, $d|bv$ donc $d|au + bv$, c'est à dire que $d|1$.
D'où: $d = \pm 1$. Donc $\delta(a,b) = \{-1; +1\} \Rightarrow a \wedge b = 1$.

$\Longrightarrow$:

Pour montrer qu'elle est nécessaire, on utilise l'**Algorithme d'Euclide**, que nous décrivons maintenant.
Si $b = 0$, alors $a \in \{-1; +1\}$ et donc $1 = a \times a + 0 \times b$.
Sinon, on effectue les divisions successives: $r_{k-1} = r_k q_k + r_{k+1}$, avec $0 \leq r_{k+1} < r_k$:

On effectue une première division euclidienne de a par $|b|$:

$$\begin{array}{c|c} r_{-1} = a & r_0 = |b| \\ \hline r_1 & q_0 \end{array}$$

On a donc: $a = |b|q_0 + r_1$. On recommence une division euclidienne, cette fois-ci, de $r_0 = |b|$ par r_1. On obtient:

$$\begin{array}{c|c} r_0 = |b| & r_1 \\ \hline r_2 & q_1 \end{array}$$

et ainsi de suite jusqu'à n le premier entier tel que: $r_{n+1} = 0$.
On peut donc rassembler toutes ces divisions sous la forme d'un tableau:

$$\begin{array}{r|c|c|c|c|c} r_{-1} = a & r_0 = b & r_1 & ... & r_n & r_{n+1} = 0 \\ \hline r_1 & q_0 & q_1 & ... & q_n & \end{array}$$

avec $0 \leq r_1 < b$, $0 \leq r_2 < r_1$ etc... ie $0 = r_{n+1} \leq r_n < ... < r_1 < b < a$

On remarque que $\delta(a,b) = \delta(r_0, r_1) = \delta(r_1, r_2) = ... = \delta(r_n, r_{n+1} = 0)$
Or, $\delta(a,b) = \{-1; +1\}$ donc $\delta(r_n = 0) = \{+1; -1\} \Longrightarrow r_n = 1$.

Montrons par récurrence que $\forall k \in [|1; n|]$, il existe $(u_k, v_k) \in \mathbb{Z}^2$ tel que:
$r_k = au_k + bv_k$
k=1: $r_1 = au_1 + bv_1$ car $a = bq_0 + r_1$, ie: $r_1 = a - bq_0$ avec $u_1 = 1$ et $v_1 = -q_0$

Récurrence: $\forall k \leq l$, a-ton $r_k = au_k + bv_k \Longrightarrow r_{l+1} = au_{l+1} + bv_{l+1}$?

$$\begin{aligned} r_{l+1} &= r_{l-1} - r_l q_l \\ &= au_{l-1} + bv_{l-1} - q_l(au_l + bv_l) \\ &= a(\underbrace{u_{l-1} - q_l u_l}_{u_{l+1}}) + b(\underbrace{v_{l-1} - q_l v_l}_{v_{l+1}}) \\ &= au_{l+1} + bv_{l+1} \end{aligned}$$

♣

Maintenant qu'on a cette relation de récurrence, pour déterminer u et v tq $au + bv = 1 (= r_n)$, on "remonte" ces divisions:

$$\begin{aligned} &1 = r_{n-2} - r_{n-1}q_{n-1} \\ &r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} && \Longrightarrow 1 = r_{n-2} - [r_{n-3} - r_{n-2}q_{n-1}] \\ &&& \Longrightarrow 1 = r_{n-2}[1 + {q_{n-1}}^2] - r_{n-3}[q_{n-1}] \\ &r_{n-2} = r_{n-4} - r_{n-3}q_{n-3} && \Longrightarrow 1 = [r_{n-4} - r_{n-3}q_{n-3}][1 + {q_{n-1}}^2] - r_{n-3}[q_{n-1}] \text{ etc...} \end{aligned}$$

et on arrive à $r_1 = a - bq_0$ que l'on remplace dans le dernier calcul.

$\Longrightarrow 1 = au + bv$ avec u et v déterminés.

C'était ***l'algorithme d'Euclide***, dit des divisions successives.

Exemple:
Montrez que $15 \wedge 11 = 1$ et déterminer une relation de Bezout.

Solution:
On effectue les divisions successives de 15 par 11:

15	11	4	3	**1**	0
	1	2	1	3	

On remonte les divisions:

$$\begin{aligned} 1 &= 4 - 3 \times 1 \\ &= \underbrace{15 - 1 \times 11}_{=4} - (\underbrace{11 - 4 \times 2}_{=3}) \\ &= 15 - 1 \times 11 - (11 - (15 - 1 \times 11) \times 2) \\ &= 15 \times 3 - 11 \times 4 \end{aligned}$$

Ainsi, 15 et 11 sont premiers entre eux, car le dernier reste non nul(ie $15 \wedge 11$) est égal à 1.
De plus, pour la relation de Bezout, on a: $u = 3$ et $v = -4$

Théorème 2.1.2 (de Gauss) *Pour tout $(a, b, c) \in \mathbb{Z}^3$, si a et b sont premiers entre eux et si $a|bc$, alors $a|c$.*

Démonstration:
Il existe $(u, v) \in \mathbb{Z}^2$, tel que $1 = au + bv$, et donc $c = acu + bcv$, comme a divise acu et a divise bcv, on en déduit que a divise leur somme c.

♣

Théorème 2.1.3 (d'Euclide) *Pour tout $(a, b) \in \mathbb{Z}^2$, si p est premier et $p|ab$, alors $p|a$ ou $p|b$.*

Démonstration:
Si p ne divise pas a, alors a et p sont premiers enre eux. Comme p divise ab, on en déduit que p divise b. ♣

2.2 Algorithme d'Euclide version matricielle

Cet algorithme d'Euclide peut être explicité de façon matricielle. L'avantage d'une telle écriture consiste à ne pas effectuer de remontée des divisions successives pour déterminer les coefficients de Bezout.

Définition 2.2.1 *Soient $x, y \in \mathbb{Z}$.*
On considère la division euclidienne de x par y et on définit 2 applications:

$$\begin{array}{rcl} \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ q : (x,y) & \longmapsto & \textit{quotient de } x \div y \\ r : (x,y) & \longmapsto & \textit{reste de } x \div y \end{array}$$

On a donc: $x = q(x,y) \times y + r(x,y)$

Démarche:
Soient $a, b \in \mathbb{N}$ tels que $a \wedge b \neq 1$, et $a = ca'$, $b = cb'$, $(a \wedge b = c$ et $a' \wedge b' = 1)$.
On cherche à simplifier la fraction $\frac{a}{b}$ et à écrire $au + bv = c$.

- <u>Etape 0:</u>
  On considère le tableau suivant:

$\times \Rsh$	$\begin{matrix} a \\ b \end{matrix}$	$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$
$\begin{matrix} 0 & 1 \\ 1 & \underbrace{-q(a,b)}_{=-q_0} \end{matrix}$		

  Et on effectue les multiplications matricielles, ce qui nous donne:

- <u>Etape 1:</u>

$\times \Rsh$	$\begin{matrix} a \\ b \end{matrix}$	$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$
$\begin{matrix} 0 & 1 \\ 1 & -q_0 \end{matrix}$	$\begin{matrix} b \\ \underbrace{a - bq(a,b)}_{=r_0} \end{matrix}$	$\begin{matrix} 0 & 1 \\ 1 & -q_0 \end{matrix}$

- Etape 2:

		b	0	1
	$\times \Rsh$	r_0	1	$-q_0$
0	1	r_0	1	$-q_0$
1	$\underbrace{-q(b, r_0)}_{=-q_1}$	$\underbrace{b - q_1 r_0}_{=r_1}$	$-q_1$	$1 + q_1 q_0$

$\vdots$

- Etape n:

		r_{n-3}	$\dots$	$\dots$
	$\times \Rsh$	r_{n-2}	u	v
0	1	c	u	v
1	$\underbrace{-q(r_{n-3}, r_{n-2})}_{=-q_{n-1}}$	$r_{n-1} = 0$	$-b'$	a'

On obtient donc directement le PGCD de a et b, les coefficients de Bezout u et v ainsi que le numérateur et le dénominateur de la fraction simplifiée. Finalement, la simplicité de cet méthode vient de la manipulation de différents produits matriciels et du résultat final qui apparaît sans avoir à effectuer une remontée des calculs. Les erreurs de calculs sont ainsi nettement limitées (expérience personnelle!).

Remarque:
Une autre version de cet algorithme consiste non pas à considérer juste q_n mais $q_n + 1$ dans les matrices de gauche, et ce, jusqu'à aboutir à un reste nul (comme cette version). Par contre, les résultats obtenus sont les mêmes, avec un signe $-$ devant (les signes de u, v, a', b' et c sont opposés) et les lignes de calculs moins nombreuses (appelons-là la version n°2).

▲

Exemple:

Déterminer une relation de Bezout entre 415 et 115.
Simplifier la fraction: $\frac{415}{115}$.

Solution:

$\Longrightarrow$ *Avec Euclide classique:*
On effectue les divisions successives de 415 par 115:

415	115	70	45	25	20	5	0
	3	1	1	1	1	4	

5 étant le dernier quotient d'une division dont le reste est nul, c'est, par définition, le PGCD de 415 et 115.
Maintenant, on remonte ces divisions:

$$\begin{aligned} 5 &= 25 - \underbrace{20 \times 1}_{=45-25} \\ &= \underbrace{25 \times 2}_{=(70-45)\times 2} -45 \\ &= 70 \times 2 - \underbrace{45 \times 3}_{=(115-70)\times 3} \\ &= \underbrace{70 \times 5}_{=(415-115\times 3)\times 5} -115 \times 3 \\ &= 415 \times 5 + 115 \times (-18) \end{aligned}$$

Donc $415 \times 5 + 115 \times (-18) = 5$, ie $u = 5, v = -18$.

$\Longrightarrow$ *Avec Euclide version matricielle* 1
On construit le tableau en suivant l'algorithme décrit précédemment (j'ai effectué les produits directement):

		415	1	0
	$\times\ \Rsh$	115	0	1
0	1	115	0	1
1	-3	70	1	-3
0	1	70	1	-3
1	-1	45	-1	4
0	1	45	-1	4
1	-1	25	2	-7
0	1	25	2	-7
1	-1	20	-3	11
0	1	20	-3	11
1	-1	5	5	-18
0	1	$\underbrace{5}_{=a\wedge b=c}$	$\underbrace{5}_{=u}$	$\underbrace{-18}_{=v}$
1	-4	0	$\underbrace{-23}_{=-b'}$	$\underbrace{83}_{=a'}$

$\Longrightarrow$ *Avec Euclide version matricielle 2*

		415	1	0
	$\times\ \Rsh$	115	0	1
0	1	115	0	1
1	-4	-45	1	-4
0	1	-45	1	-4
1	3	-20	3	-11
0	1	-20	3	-11
1	-2	-5	-5	18
0	1	$\underbrace{-5}_{=-a\wedge b=c}$	$\underbrace{-5}_{=-u}$	$\underbrace{18}_{=-v}$
1	-4	0	$\underbrace{23}_{=b'}$	$\underbrace{-83}_{=-a'}$

Toutes ces différentes versions de l'algorithme d'Euclide ont été appliquées avec des nombres **entiers**. Mais on constatera plus loin qu'elles sont également appliquables dans la cas de fonctions polynômiales. Les calculs seront basés sur les divisions polynômiales dont je rappellerai le mode de fonctionnement.

2.3 Applications

2.3.1 Résolution de $au + bv = c$; $a, b, c, u, v \in \mathbb{Z}^*$

Démarche:

Soit $d = a \wedge b$.

- Si $d \nmid c$, alors l'équation n'a pas de solution car sinon, on aurait:
  si $a = a'd$, $b = b'd$, avec $a', d, b' \in \mathbb{Z}^*$, alors $(a'u + b'v) \times d = c \Longrightarrow d|c$.

- On est donc dans le cas où $d|c$.

Notons $c = dc'$, $c \in \mathbb{Z}^*$. $au + bv = c$ $(\star)$ $\Longrightarrow a'du + b'dv = c'd$
$\Longrightarrow a'u + b'v = c'$ avec $a' \wedge b' = 1$

Par **Bezout**, comme a' et b' sont premiers entre eux, il existe (u_0, v_0) tel que

$$a'u_0 + b'v_0 = 1(\star\star)$$

On trouve (u_0, v_0) tout simplement en appliquant **l'agorithme d'Euclide**.

En multipliant $(\star\star)$ par c', on obtient : $a'c'u_0 + b'c'v_0 = c'$.
Alors $a'u + b'v = c'$ a pour solution particulière: $(c'u_0, c'v_0)$, notée $(\overline{u}_0, \overline{v}_0)$

► Soit (u, v) une autre solution. Par identification, on a:
$a'u + b'v = c' = a'\overline{u}_0 + b'\overline{v}_0$
$\Longrightarrow a'(u - \overline{u}_0) + b'(v - \overline{v}_0) = 0$
$\Longrightarrow a'(u - \overline{u}_0) = -b'(v - \overline{v}_0)$

Or, $a' \wedge b' = 1$ $\Longrightarrow$ (par *Gauss*) $b'|(u - \overline{u}_0)$
$\Longrightarrow u - \overline{u}_0 = kb'k \in \mathbb{Z}^*$
$\Longrightarrow \boxed{u = \overline{u}_0 + kb'}$

Donc: $a'kb' + b'(v - \overline{v}_0) = 0 \Longrightarrow \boxed{v = \overline{v}_0 - ka'}$

Finalement: $S = \{(c'u_0 + kb', c'v_0 - ka'), k \in \mathbb{Z}\}$

Remarque:
Pour résoudre l'équation $ax + by = c$ avec $(a \wedge b) = c$, c'est extrêmement simple: on applique l'algorithme d'Euclide. ▲

Exemple:

1) Résoudre l'équation $151u_0 + 77v_0 = 1$ $(\star)$:

Effectuons les divisions successives de 151 par 77:

151	77	74	3	2	1	0
	1	1	24	1	2	

Remarquons que $(u, v) = (5u_0, -5v_0)$ sera solution de $(\star)$ car:

$$\begin{aligned} 151u - 77v &= 151 \times 5 \times u_0 + 77 \times 5 \times v_0 \\ &= 5 \times (151u_0 + 77v_0) \\ &= 5 \end{aligned}$$

On remonte les calculs:

$$\left.\begin{aligned} 1 &= 3 - 2 \times 1 \\ 2 &= 74 - 3 \times 24 \\ 3 &= 77 - 74 \times 1 \\ 74 &= 151 - 77 \times 1 \end{aligned}\right. \Longrightarrow 1 = \underbrace{51}_{v_0} \times 77 + 151 \times \underbrace{(-26)}_{u_0}$$

Une solution de $(\star)$ est donc $(u_0, v_0) = (-26, 51)$

2) Résoudre l'équation $151u - 77v = 5$ $(\star\star)$:

Par la remarque de cette $1^{\text{ère}}$partie, on obtient une solution de $(\star\star)$:

$(5 \times (-26), -5 \times 51) = (130, -255)$

Soit (u', v') une autre solution de$(\star)$. On a alors

$$\begin{cases} 151u - 77v = 5 & \text{donc } u' = u - 77k \\ 151u' - 77v' = 5 & \text{donc } v' = v - 151k \end{cases}$$

Finalement, les solutions de $(\star\star)$ ***sont:***

$$S = \{(-130 - 77k, -255 - 151k), k \in \mathbb{Z}\}$$

2.3.2 Réduction en éléments simples

Le but d'une décomposition en éléments simples est le suivant:

On se donne une fraction du type $\frac{P}{AB}$, et on cherche à se ramener à une somme de fractions telle que $\frac{P}{AB} = \frac{P_1}{A} + \frac{P_2}{B}$, où P, P_1, P_2, A et B sont des polynômes finis.

Démarche:
Par l'algorithme d'Euclide, on résoud une équation du type: $AU + BV = 1$, où U et V sont également des polynômes.
Pour cela, on utilise la version matricielle d'Euclide qui facilite énormément les calculs lors de divisions et multiplications polynômiales.
Ainsi, on arrive à : $\boxed{\frac{P}{AB}} = \frac{P\times 1}{AB} = \frac{P(AU+BV)}{AB} = \frac{PAU}{AB} + \frac{PBV}{AB} = \boxed{\frac{PU}{B} + \frac{PV}{A}}$

Rappel:
Comment effectuer une division de $A = ax^2 + bx + c$ par $B = dx + f$?

- *Première étape:*

$$\begin{array}{c|l} ax^2 + bx + c & dx + f \\ \hline [ax^2 - dx(\frac{ax}{d})] + [bx - f(\frac{ax}{d})] + c & \frac{ax}{d} (= \frac{ax^2}{dx}) \end{array}$$

- *Deuxième étape:*

$$\begin{array}{c|l} 0 + (b - f\frac{a}{d})x + c & dx + f \\ \hline \underbrace{[(b - f\frac{a}{d})x - dx(\frac{db - fa}{d^2})]}_{=0} + [c - f(\frac{db-fa}{d^2})] & \frac{db-fa}{d^2} (= \frac{(b-f\frac{a}{d})x}{dx}) \end{array}$$

- *Dernière étape:*

$$\underbrace{ax^2 + bx + c}_{A} = \underbrace{(dx + f)}_{B} \underbrace{[(\frac{ax}{d}) + (\frac{db - fa}{d^2})]}_{quotient} + \underbrace{c - f(\frac{db - fa}{d^2})}_{reste}$$

On généralise tout simplement ce type de division à des polynômes de degrés supérieurs à 2, en considérant étape par étape la division de chaque monôme de A par le polynôme B tout entier (A étant le polynôme de degré supérieur), jusqu'à aboutir à un reste dont le degré est strictement inférieur à celui du diviseur B. ⋇

Exemple:
Considérons le polynôme défini par:

$$Q(x) = \frac{-55x^4 + 25x^3 + 9x^2 + 40x + 61}{(x - 1)^2(x - 2)^3}$$

et réduisons-le en éléments simples.
On pose $A = (x - 2)^3, B = (x - 1)^2$, et $P = -55x^4 + 25x^3 + 9x^2 + 40x + 61$.

Déterminons une relation de Bezout entre A et B, ie, cherchons U et V tels que: $AU + BV = 1$.
Tout d'abord, $(x-1)^2 = x^2 - 2x + 1$ et $(x-2)^3 = x^3 - 6x^2 + 12x - 8$.

▶ On va d'abord procéder à une division Euclidienne de A par B comme application directe des divisions polynômiales:

$$\begin{array}{r|l} x^3 - 6x^2 + 12x - 8 & x^2 - 2x + 1 \\ \hline 0 - 4x^2 + 11x - 8 & x - 4 \\ 0 + 3x - 4 & \end{array}$$

$\Longrightarrow$ Le quotient est donc égal à $x-4$ et le reste égal à $3x-4$.

On recommence: $$\begin{array}{r|l} x^2 - 2x + 1 & 3x - 4 \\ \hline 0 - \frac{2x}{3} + 1 & \frac{x}{3} - \frac{2}{9} \\ 0 + \frac{1}{9} & \end{array}$$

$\Longrightarrow$ Le nouveau quotient est égal à $\frac{x}{3} - \frac{2}{9}$ et le reste $\frac{1}{9}$. On multiplie le tout par 9 afin de se ramener à des entiers.

Et ainsi de suite jusqu'au premier reste nul.

▶ Effectuons maintenant la version matricielle d'Euclide: notons auparavant la présence du "multiplicateur" dans la colonne de gauche qui permet de lever les fractions.

		$x^3 - 6x^2 + 12x - 8$	1	0
	$\times \Rsh$	$x^2 - 2x + 1$	0	1
0	1	$x^2 - 2x + 1$	0	1
1	$-x + 4$	$3x - 4$	1	$-x + 4$
0	1	$3x - 4$	1	$-x + 4$
$\underbrace{9}_{=multiplicateur}$	$-3x + 2$	1	$-3x + 2$	$3x^2 - 14x + 17$
0	1	$\underbrace{1}_{=A\wedge B}$	$\underbrace{-3x + 2}_{=U}$	$\underbrace{3x^2 - 14x + 17}_{=V}$
1	$-3x + 4$	0	$9x^2 - 18x$	$-9x^3 + 54x^2 - 108x + 72$

Ainsi, on trouve que:
$AU + BV = 1 = (x-2)^3 \times (-3x + 2) + (x-1)^2 \times (3x^2 - 14x + 17)$

Et donc:

$$\begin{aligned} Q(x) &= \frac{PU}{B} + \frac{PV}{A} \\ &= \frac{(-55x^4+25x^3+9x^2+40x+61)(-3x+2)}{(x-1)^2} + \frac{(-55x^4+25x^3+9x^2+40x+61)(3x^2-14x+17)}{(x-2)^3} \end{aligned}$$

2.3.3 Systèmes de congruences

Définition 2.3.1 (Congruence)

Résolution d'un système de congruences du type:

$$(\bigstar)\begin{cases} x \equiv a \bmod b \\ x \equiv a' \bmod b' \end{cases}$$

- Cas où $b \wedge b' = 1$:
  On sait que $b \wedge b' = 1$, donc par **Bezout**, il existe $u, v \in \mathbb{Z}$ tels que: $bu + b'v = 1$.

  $$\Longrightarrow \begin{cases} b'v & \equiv 1 \bmod b \\ bu & \equiv 1 \bmod b' \end{cases}$$

  $$\text{ie : } \begin{cases} ab'v & \equiv a \bmod b \\ a'bu & \equiv a' \bmod b' \end{cases}$$

  On obtient: $\boxed{x = ab'v + a'bu}$

  $$\begin{aligned} \overline{x}^b &= \overline{ab'v + a'bu}^b \\ &= \overline{ab'v}^b + \overline{a'bu}^b \\ &= \overline{a(1-bu)}^b + \overline{a'u}^b.\overline{b}^b \\ &= \overline{a}^b.\overline{1}^b + \overline{a'u}^b.\overline{0}^b \\ &= \overline{a}^b \end{aligned}$$

  De même, $\overline{x}^{b'} = \overline{ab'v + a'bu}^{b'} = \overline{a'}^{b'}$
  On a donc bien $x = ab'v + a'bu$ qui vérifie le système de congruence:

  $$\begin{cases} x \equiv a \bmod b \\ x \equiv a' \bmod b' \end{cases}$$

Soit x' une autre solution:
$x \equiv a \bmod b \Rightarrow x' \equiv a \bmod b$, donc $x - x' \equiv 0 \bmod b \Rightarrow x - x' \in b\mathbb{Z}$
De même:
$x - x' \equiv 0 \bmod b' \Rightarrow x - x' \in b\mathbb{Z}$
$\Rightarrow (x - x') \in (b\mathbb{Z} \cap b'\mathbb{Z}) = ppcm(b, b')\mathbb{Z} = bb'\mathbb{Z}$ car $b \wedge b' = 1$
On obtient alors: $\boxed{x' \equiv x \bmod bb'}$

Finalement, les solutions de ce système sont:

$$S = \{ab'v + a'bu + kbb', k \in \mathbb{Z}\}$$

- Cas où b et b' sont quelconques:
  Soit $d = b \wedge b'$, alors on a; $b = db_1, b' = db'_1$ et par **Bezout**, il existe $(u_1, v_1) \in \mathbb{Z}$ tels que: $b_1u_1 + b'_1v_1 = 1$

$$\begin{cases} x & \equiv & a & \bmod & b \\ x & \equiv & a' & \bmod & b' \\ a' - a & \equiv & 0 & \bmod & d \end{cases}$$

Si x est solution de ($\bigstar$), alors;

$$\begin{array}{ll} x = a + bk & = a + db_1k \\ x = a' + b'k' & = a' + db'_1k' \end{array} \Longrightarrow a - a' = d(-kb_1 - k'b'_1)$$

Pour que x existe, d doit diviser $a' - a$
Si $d \nmid a' - a$, alors il n'y a pas de solutions.
Si $d \mid a' - a$, alors $a' - a = d'd$ avec $d' \in \mathbb{Z}$

On pose alors:

$$y = \frac{x - a}{d}, \ (y \in \mathbb{Z} \text{ car } d \mid x - a) \Rightarrow \begin{cases} y & \equiv & 0 & \bmod & b_1 \\ y & \equiv & d' & \bmod & b'_1 \end{cases}$$

On s'est ainsi ramené à $b_1 \wedge b'_1 = 1$.
On applique alors l'algorithme du cas où $b \wedge b' = 1$.
On trouve ensuite y et donc, $x = dy + a$.

Exemple:

1. <u>Résoudre</u>:

$$\begin{cases} x \equiv 5 \text{ mod } [33] \\ x \equiv 20 \text{ mod } [35] \end{cases}$$

▶ On effectue les divisions successives de 35 par 33:

$$\begin{array}{c|c|c|c|c} 35 & 33 & 2 & 1 & 0 \\ \hline & 1 & 16 & 2 & \end{array} \Rightarrow 1 = 33(17) + 35(-16), \text{ ie: } u = 17 \text{ et } v = -16.$$

On a une première solution:
$x = 20 \times 33(-16) + 5 \times 35 \times (17)$, et donc:

$$S = \{335 + 1155k, k \in \mathbb{Z}\}$$

2. <u>Résoudre</u>:

$$\begin{cases} x \equiv 5 \text{ mod } [132] \\ x \equiv 20 \text{ mod } [140] \end{cases}$$

▶ On effectue les divisions successives de 140 par 132:

$$\begin{array}{c|c|c|c|c} 140 & 132 & 8 & 4 & 0 \\ \hline & 1 & 16 & 2 & \end{array}$$

Or, $140 \wedge 132 = 4$, et $4 \nmid (20 - 5)$. Donc pas de solution.

3. <u>Résoudre</u>:

$$\begin{cases} x \equiv 3 \text{ mod } [4] \\ x \equiv -2 \text{ mod } [3] \\ x \equiv 7 \text{ mod } [5] \end{cases}$$

Considérons:

$$(1) \begin{cases} x \equiv 1 \text{ mod } [4] \\ x \equiv 0 \text{ mod } [3] \\ x \equiv 0 \text{ mod } [5] \end{cases} (2) \begin{cases} x \equiv 0 \text{ mod } [4] \\ x \equiv 1 \text{ mod } [3] \\ x \equiv 0 \text{ mod } [5] \end{cases} (3) \begin{cases} x \equiv 0 \text{ mod } [4] \\ x \equiv 0 \text{ mod } [3] \\ x \equiv 1 \text{ mod } [5] \end{cases}$$

On va résoudre chaque système 1 à 1.

$$(1) \Leftrightarrow \begin{cases} x \equiv 1 \text{ mod } [4] \\ x \equiv \text{mod}[15] \end{cases}$$

$$\begin{array}{c|c|c|c|c} 15 & 4 & 3 & 1 & 0 \\ \hline & 3 & 1 & 3 & \end{array} \Rightarrow 1 = 4 \times 4 - 15 \text{ donc } \boxed{x_1 \equiv -15 \text{ mod } [60]}$$

$$(2) \Leftrightarrow \begin{cases} x \equiv 1 \text{ mod } [3] \\ x \equiv 0 \text{ mod } [20] \end{cases}$$

$$\begin{array}{c|c|c|c|c} 20 & 3 & 2 & 1 & 0 \\ \hline & 6 & 1 & 2 & \end{array} \Rightarrow 1 = 3 \times 7 - 20 \text{ donc } \boxed{x_2 \equiv -20 \text{ mod } [60]}$$

$$(3) \Leftrightarrow \begin{cases} x \equiv 1 \text{ mod } [5] \\ x \equiv \text{mod}[12] \end{cases}$$

$$\begin{array}{c|c|c|c|c} 12 & 5 & 2 & 1 & 0 \\ \hline & 2 & 2 & 2 & \end{array} \Rightarrow 1 = 5 \times 5 - 12 \times 2 \text{ donc } \boxed{x_3 \equiv -24 \text{ mod } [60]}$$

Solution finale:

$$\begin{aligned} x &= 3x_1 - 2x_2 + 7x_3 \\ &= (-3 \times 15 + 2 \times 20 - 7 \times 24) \text{ mod } [60] \\ &= (-45 + 40 - 168) \text{ mod } [60] \\ &= -173 \text{ mod } [60] \end{aligned}$$

$$\boxed{x \equiv -173 \text{ mod } [60]}$$

Chapter 3

Euclide non classique

3.1 Fractions continues

Chapter 4

D'Euclide à Padé