M1 MINT – Université Paris-Saclay

– MAO – Algèbre avec SAGE

N. Perrin

Université de Versailles Saint-Quentin-en-Yvelines
Année 2017-2018

Ce cours est une introduction au calcul formel avec une partie pratique qui utilise le logiciel SAGE.

Le calcul formel calcule des objets mathématiquement *exacts* par opposition au calcul aproché dont il est question dans le seconde partie de ce cours (second partie enseignée par Tahar Boulmezaoud). On va y considérer deux aspects importants du calcul formel

1. la “calculabilité” et
2. la “complexité”.

La calculabilité comme son nom l'indique cherche à déterminer si un calcul est réalisable par une machine. Il s'agira donc dans un premier temps de fournir un algorithme de calcul puis de l'implémenter, dans un laguage, afin de la faire tourner sur machine (et de vérifier qu'il fait bien ce qu'on lui demande !).

La complexité étudie les algorithmes obtenus à l'étape précédente et évalue le temps de calcul. On cherche bien sûr à réaliser des algorithmes qui soient les plus rapides possibles.

Table des matières

Première partie .

Arithmétique des grands entiers et des polynômes

1. Représentation des grands entiers

Avant même de pouvoir commencer à concevoir des algorithmes et écrire des programmes, un point imporant est de comprendre les objets que l'on manipule. Les plus simples sont les entiers. Mais attention, on a dit que l'on voulait faire des calculs exacts et ce quels que soient les entiers et notamment *quelque soit leur taille*. Ceci peut poser un problème comme le montre l'exemple suivant (cf. feuille de TD 1).

Exemple 1.0.1 On tape la commande suivante dans SAGE qui nous renvoie :

```
sage: 10^50 + 1. - 10^50
...: 0.000000000000000
```

Le problème ici est que le fait d'avoir entré 1. impose à SAGE de se placer dans les nombres réels qui sont toujours approchés (avec 53 bits de précision par défaut). Cette précision n'est pas assez grande pour notre calcul et SGAE ne "voit" plus le +1. On obtient 0. Si par contre on tape la commande suivante SAGE renvoie :

```
sage: 10^50 + 1 - 10^50
...: 1
```

SAGE a maintenant fait un calcul formel comme nous le faisons nous même et a simplifié les deux 10^{50}.

Un autre exemple : sage peut traiter des entiers aussi grand qu'on le veut. Les seules limites sont la places dans la machines et le temps.

Exemple 1.0.2 Voici quelques résultats de calcul de puissance de 2 avec SAGE :

```
sage: 2^100
...: 1267650600228229401496703205376

sage: 2^1000
...: 10715086071862673209484250490600018105614048117055336074437503883703510511249361224931983788156958581275946729175531468251871452856923140435984577574698574803934567774824230985421074605062371141877954182153046474983581941267398767559165543946077062914571196477686542167660429831652624386837205668069376
```

On que que même si le calcul est instantanné avec SAGE, c'est vite la place qui va manquer...

Comment gère-t-on les entiers de tailles arbitraires ? L'ordinateur en tant que machine ne peut traiter que des objets de tailles finie. En général, le processeur peux gérer des données de 32 ou de 64 bits. Si on transforme ces bits en entiers, on peut avoir des entiers de tailles maximale 2^{64} traités par l'ordinateur. Or on vient de voir que sage nous donne immédiatement les valeurs de 2^{100} ou même 2^{1000} (et même $2^{1000000}$ à partir duquel sage n'affiche plus toute la réponse). Par exemple pour $2^{10000000}$ si on utilise la commande `%\time` on obtient la reponse suivante de sage :

```
...: CPU time: 0.86 s, Wall time: 1.07 s
```

ce qui signifie que SAGE a mis 1,07 secondes pour faire le calcul (et 0,86 secondes pour le processeur.

Comment un ordinateur gère-t-il les grand entiers (bien plus grands que la taille de son processeur) ? Il procède exactement comme nous : il les découpe en morceaux (comme l'écriture en base 10) avec des chiffres. L'ordinateur va écrire en base 2^{32} ou 2^{64} selon la taille de son processeur (32 ou 64 bits). On va dans la suite se placer dans le cas de processeurs de 64 bits.

Définition 1.0.3 Entiers machine et multiprécision.

1. Un **entier machine** est un nombre entier que le processeur de la machine peut gérer directement. C'est donc un entier de taille 2^{64} (64 bits).

2. Un **entier multiprécision** a est un nombre entier (beaucoup) plus grand qu'un entier machine. On l'écrit en base 2^{64} sous la forme suivante :

$$a = (-1)^s \sum_{i=0}^{n} a_i 2^{64i},$$

où $s \in \{0; 1\}$ est le signe de l'entier a, n est un entier machine tel que $0 \leq n+1 < 2^{63}$, c'est la **taille** de a et les a_i sont des entiers machines. On code également la taille et le signe de a dans les premiers bits. L'entier a sera donc une suite d'entiers machines :

$$a = (s', a_0, \cdots, a_n)$$

où $s' = s \cdot 2^{63} + n + 1$.

Remarque 1.0.4 Comme on a $0 \leq n + 1 < 2^{63}$, la valeur de s' permet de retrouver à la fois celle de s et celle de n et donc le signe et la taille de notre entier. En effet, on a

— Si $s' = s \cdot 2^{63} + n + 1 < 2^{63}$ alors $s = 0$ et $n + 1 = s \cdot 2^{63} + n + 1 = s'$

— Si $s' = s \cdot 2^{63} + n + 1 \geq 2^{63}$ alors $s = 1$ et $n + 1 = s \cdot 2^{63} + n + 1 - 2^{63} = s' - 2^{63}$

Exemple 1.0.5 L'entier 1 s'écrit $(1,1)$ c'est-à-dire $s'=1$ et donc $s=0$ et $n=0$. On a aussi $a_0=1$.

L'entier -1 s'écrit $(2^{63}+1,1)$ c'est-à-dire $s'=2^{63}+1$ et donc $s=1$ et $n=0$. On a aussi $a_0=1$.

Par convention l'entier 0 s'écrit (0).

Il est souvent très utile de connaitre la taille de l'entier à l'avance (d'où l'entier machine qui donne n). Comme on se limite pour n à un entier machine, ceci donne tout de même une limite aux entiers multiprécisions.

Proposition 1.0.6 Un entier multiprécision est compris dans l'intervalle

$$[-2^{64\cdot 2^{63}}+1, 2^{64\cdot 2^{63}}-1].$$

Preuve. Exercice. ∎

Pour stocker les plus grands entiers multiprécision, il faut tout de même 1^{11} GB (Gigas) ou encore 10^8 TB (Teras) ce qui représente plus de 1 millions de diques de 1 To chacun à plus de 500 euros donc un coup de plus 500 millions d'euros pour stocker de tels entiers (sans compter la place prise par ces disques de stockage...).

Remarque 1.0.7 On peut retrouver n à partir de a de la manière suivante

$$n = \lfloor \log_{2^{64}} |a| \rfloor - 1 = \left\lfloor \frac{\log_2 |a|}{64} \right\rfloor - 1.$$

Le nombre d'entiers machines nécessaires à décrire a est $\lambda(a) = n+2$.

2. Addition

2.1. Additionner les entiers multiprécisions

Dans cet paragraphe, nous allons donner un algorithme rudimentaire pour expliquer comment l'ordinateur gère l'additions d'entiers multiprécision. Pour celà, on suppose que notre processeur est capable d'additionner deux entiers machines. Plus précisément, on suppose que notre processeur dispose de l'opération suivante

$\texttt{ADDITION}(a, b) = (c, \gamma)$

Ici, les entrées a et b sont des entiers machines *i.e* $a, b \in [0, 2^{64} - 1]$ et la sortie (c, γ) est une paire formée d'un entier machine c d'un bit $\gamma \in \{0; 1\}$ (la retenue). La formule qui définit (c, γ) est la suivante :

$$a + b = \gamma \cdot 2^{64} + c.$$

Nous nous contenterons de donner un algorithme qui additionne des entiers multiprécisions sans signe et de la même taille. Nos entiers sont donc de la forme $a = (n + 1, a_0, \cdots, a_n)$ et $b = (n+1, b_0, \cdots, b_n)$.

Algorithme 2.1.1 (Addition des entiers multiprécisions)

$\gamma_0 := 0$
`For` i `in range` $(0, n + 1)$`:`
    (d_i, α_i) :=`ADDITION`(a_i, b_i)
    (c_i, β_i) :=`ADDITION`(d_i, γ_i)
    $(c_i, \gamma_{i+1}) := (c_i, \alpha_i + \beta_i)$
$c_{n+1} := \gamma_{n+1}$
`If` $c_{n+1} \neq 0$ `and` $n + 2 = 2^{63}$ `return` Somme trop grande !
`If` $c_{n+1} \neq 0$ `and` $n + 2 < 2^{63}$ `return` $(n + 2, c_0, \cdots, c_{n+1})$
`If` $c_{n+1} = 0$ `return` $(n + 1, c_0, \cdots, c_n)$

Exemple 2.1.2 Pour illustrer l'algorithme ci-dessus, nous allons faire une addition en base 10 (et pas 2^{64}) de deux entiers. On se propose de faire l'opération

$$8438 + 1945$$

avec $a = 8438 = (4; 8, 3, 4, 8)$ et $b = 1945 = (4; 5, 4, 9, 1)$ (le premier terme est la taille). On représente les étapes de l'algorithme dans un tableau

i	0	1	2	3	4
a_i	8	3	4	8	
b_i	5	4	9	1	
d_i	3	7	3	9	
α_i	1	0	1	0	
c_i	3	8	3	0	1
β_i	0	0	0	1	0
γ_i	0	1	0	1	1

On obtient

$$8438 + 1945 = 10383.$$

Exercice 2.1.3 Écrire un algorithme qui permet d'additionner des entiers multiprécisions quelconques (avec signes et de tailles différentes).

Proposition 2.1.4 L'algorithme d'addition des entiers multiprécisions de taille n et sans signe utilise exactement $2(n + 1)$ operations processeur `ADDITION`.

Preuve. On fait deux `ADDITIONS` pour chaque entier i entre 0 et n. ∎

Exercice 2.1.5

1. Écrire un programme qui fait passer un entier dans sa représentation en tant qu'entier multiprécision ainsi qu'on programme qui fait l'inverse.

2. Écrire un programme qui fait l'addition des entiers multiprécisions et tester s'il fonctionne grâce au programme précédent.

Simplification : Pour éviter d'avoir à tester des entiers trop grands, on pourra aussi réaliser les programmes ci-dessus avec des entiers machines de 1 bits (et donc on écrit les entiers en base 2).

Remarque 2.1.6 La retenue qu'on a gérée avec les paramètres γ_i ci-dessus complique le calcul d'efficacité (ou de complexité) de cet algorithme. Pour évaluer la complexité, on va utiliser un modèle plus simple : les polynômes.

2.2. Addition des polynômes

À la place des entiers, on va maintenant considérer les polynômes en une variable x. Il peut sembler que ceci introduit de la complexité mais il n'en sera rien : on va grâce à cette astuce s'éviter toute retenue dans les opérations arithmétiques.

Définition 2.2.1 Un **polynôme de grand degré** sur un anneau A est la donnée

$$p(x) = \sum_{i=0}^{n} a_i x^i$$

où les a_i sont des éléments de A et n est un entier appelé **degré ou taille**. Pour la machine le polynôme est représenté par $(n, a_0, \cdots, a_n)$.

Remarque 2.2.2 Si on remplace x par 2^{64} et A par les entiers machines, on retrouve l'écriture des entiers multiprécision. L'arithmétique des (addition, soustraction, multiplication et division) entiers et des polynômes sont très semblable mais celle des polynômes est un peu plus simple : il n'y a jamais de retenue. On va donc utiliser cette dernière pour les calculs de complexité. Dans beaucoup de situations les calculs de complexité pour les entiers donnent des résultats semblables à ceux de polyômes.

L'opération `ADDITION` sera remplacée par l'addition dans l'anneau A. Encore une fois, on va supposer que nos polynômes ont le même degré. C'est un exercice facile que d'adapter l'algorithme suivant au cas général. On suppose donc que a et b sont de la forme $a = (n, a_0, \cdots, a_n)$ et $b = (n, b_0, \cdots, b_n)$.

Algorithme 2.2.3 (Addition des polynômes)

`For` i `in range` $(0, n+1)$`:`
    $c_i := a_i + b_i$
`return` $(n, c_0, \cdots, c_n)$

Proposition 2.2.4 L'algorithme d'addition des polynômes de taille n utilise exactement $n+1$ additions dans A.

Preuve. On fait une addition pour chaque entier i entre 0 et n. ∎

L'opération d'addition n'est donc pas une opération très coûteuse : de l'ordre de la taille des objets à additionner. L'opération importante en arithmétique et qui peut être très couteuse en temps est la multiplication.

2.3. Polynômes et sage

Pour travailler avec des polynômes dans sage, c'est assez simple. Pour définir une variable x ou y dans sage, on tape en général la commande :

```
sage: x = var('x') ; y = var('y')
```

On effectue alors des calculs sur des expressions formelles. Par exemple

```
sage: x = var('x') ; p = (2*x+1)*(x+2)*(x^4-1)
```

On dispose pour ces expressions une fonction degré :

```
sage: p.degree(x)
 ...: 6
```

mais sage ne change pas l'expression pour la représenter :

```
sage: p
 ...: (2*x+1)*(x+2)*(x^4-1)
```

Sage permet de traiter les polynômes de façon plus algébrique et calculer comme dans l'anneau des polynômes $R = A[x]$ par exemple avec $A = \mathbb{Q}$, $A = \mathbb{R}$ ou encore $A = \mathbb{Z}/4\mathbb{Z}$. Pour les polynômes à coefficients dans $\mathbb{Q}$ (qui est représenté par `QQ` dans sage). On tape :

```
sage: x = polygen(QQ,'x')
```

Si maintenant on considère le même polynôme, sage dévelope automatiquement le polynôme. La fonction degré fonctionne toujours :

```
sage: p = (2*x+1)*(x+2)*(x^4-1) ; p ; p.degree()
 ...: 2*x^6 + 5*x^5 + 2*x^4 - 2*x^2 - 5*x - 2
 ...: 6
```

Pour construire l'anneau $R = \mathbb{Q}[x]$, on tape :

```
sage: R = PolynomialRing(QQ,'x') ; R
 ...: Univariate Polynomial Ring in x over Rational Field
```

3. Multiplication

Comme on vient de le voir. Les algorithmes et le calcul de la complexité sont souvnt plus facile avec les polynômes qu'avec les entiers multiprécisions même s'ils sont de nature semblable. Nous allons donc commencer par nous intéresser au cas de la multiplication des polynômes.

Nous donnons ici l'algorithme naif de multiplication de deux polynômes $a = \sum_{i=0}^{n} a_i x^i$ et $b = \sum_{i=0}^{m} b_i x^i$ avec $m \leq n$

Algorithme 3.0.1 (Algorithme "naif" de multiplication des polynômes)

`For` k `in range` $(0, n+m+1)$:
    $c_k := 0$
    `For` i `in range` $(\max(0, k-m), \min(k, n)+1)$:
        $c_k = c_k + a_i b_{k-i}$

`Return` $\sum_{k=0}^{n+m} c_k x^k$.

Proposition 3.0.2 Pour multiplier deux polynômes de degrés n et m, l'algorithme naïf nécessite $(m+1)(n+1)$ additions et $(m+1)(n+1)$ multiplications.

Preuve. On effectue deux boucles et pour chaque boucle on doit faire une addition et une multiplication. On doit donc effectuer la somme suivante

$$S = \sum_{k=0}^{n+m} \sum_{i=\max(0,k-m)}^{\min(k,n)} 1.$$

On coupe la première somme en trois afin de calculer cette double somme correctement. Pour celà on distingue trois cas : $k \in [0, m-1]$ ou $k \in [m, n]$ ou $k \in [n, n+m]$. Dans le premier cas on calcule la somme

$$S_1 = \sum_{k=0}^{m-1} \sum_{i=0}^{k} 1 = \sum_{k=0}^{m-1} (k+1) = \frac{m(m+1)}{2}.$$

Dans le second cas

$$S_2 = \sum_{k=m}^{n} \sum_{i=k-m}^{k} 1 = \sum_{k=m}^{n} (m+1) = (m+1)(n-m+1).$$

Dans le dernier cas

$$S_3 = \sum_{k=n+1}^{n+m} \sum_{i=k-m}^{n} 1 = \sum_{k=n+1}^{n+m} (n+m+1-k) = m(n+m+1) - \frac{(n+m+1)(n+m)}{2} + \frac{n(n+1)}{2}.$$

On obtient $S = S_1 + S_2 + S_3 = (m+1)(n+1)$. ∎

On peut sans trop réfléchir faire un peu mieux. Pour celà on remarque que faire un produit d'un scalaire a_k par un polynôme $b = \sum_{i=0}^{m} b_i x^i$ nécessite $m+1$ multiplications :

$$a_k \cdot b = \sum_{i=0}^{m} a_k b_i x^i.$$

On peut alors proposer un nouvel algorithme.

Algorithme 3.0.3 (Algorithme "naif amélioré")

`For` k `in range` $(0, n+1)$`:`
    $d_k := (a_k \cdot b)x^k$

`Return` $\sum_{k=0}^{n} d_k$.

Proposition 3.0.4 Pour multiplier deux polynômes de degrés n et m, l'algorithme naïf amélioré nécessite au plus mn additions et $(m+1)(n+1)$ multiplications.

Preuve. À chaque tour de boucle on fait une opération $a_k \cdot b$ qui nécessite $m+1$ multiplications. La multiplication par x^i ne coute rien, c'est juste un décalage dans les coefficients. On a donc $(n+1)(m+1)$ multiplications. On a ensuite n additions de polynômes. En regardant de près, on voit qu'à chaque étape, on ne doit faire que m additions pour sommer ces polynômes car ils sont "décalés :

$$\begin{array}{ccccccccc} a_{k+1}b_m x^{m+k+1} & + & a_{k+1}b_{m-1}x^{m+k} & + & \cdots & + & a_{k+1}b_0 x^{k+1} & & \\ & & a_k b_m x^{m+k} & + & \cdots & + & a_k b_1 x^{k+1} & + & a_k b_0 x^k \end{array}$$

ce qui donne nm additions. ∎

Corollaire 3.0.5 Les algorithmes naifs permettent de multipler des polynômes de degrés n et m en au plus $2nm + n + m + 1$ opérations soit en $O(nm)$.

L'avantage du second algorithme est de permettre d'écrire un algorithme pour les entiers sans avoir à prendre en compte les retenues. On écrit nos entiers sous la forme $a = \sum_{i=0}^{n} a_i 2^{64i}$ et $b = \sum_{i=0}^{m} b_i 2^{64i}$ avec $m \leq n$. On commence par définir

$$a_k \cdot b = \sum_{i=1}^{m} a_k b_i 2^{64i}.$$

Ici on aurait besoin d'être plus précis et de prendre en compte les retenues : le produit de deux entiers machines $a_k b_i$ peut dépasser la taille des entiers machine.

Algorithme 3.0.6 (Algorithme "naif" de multiplication des entiers)

`For` k `in range` $(0, n+1)$:
$d_k := (a_k \cdot b)2^{64k}$

`Return` $\sum_{k=0}^{n} d_k$.

Proposition 3.0.7 Pour multiplier deux entiers multiprécisions de tailles n et m, l'algorithme naïf amélioré nécessite au plus $O(mn)$ opérations processeur.

Exercice 3.0.8 Donner un algorithme qui permette d'écrire l'opération $a_k \cdot b$ ci-dessus et évaler la complexité de l'algorithme naif utilisant cet algorithme.

Remarque 3.0.9 On voit que la multiplication est beaucoup plus "coûteuse" que l'addition. Il va donc falloir chercher à minimiser le nombre de multiplications dans les algorithmes ainsi qu'améliorer l'algorithme de multiplication. On vera des algorithmes plus efficaces pour la multiplication par la suite, notamment l'algorithme de Karatsuba et la transformation de Fourier discrète.

4. Division euclidienne

La division euclidienne outre son intérêt intrinsèque est très utile dans de nombreuses situations :

- test d'exactitude : pour vérifier que deux entiers a et b sont égaux, on vérifie que $a \equiv b \pmod{n}$.
- en cryptographie (code RSA par exemple)
- pour l'acceleration des algorithmes de multiplication.

Remarque 4.0.1 Pour les entiers, la division euclidienne est bien définie. Par contre, pour les polynômes $A[x]$ à coefficients dans un anneau A, la division euclidienne n'est pas bien définie. On a alors deux alternatives :

- choisir pour A un corps, la division euclidienne existe alors toujours,
- ne faire que des division par des polynômes dont le coefficient dominant est inversible.

C'est cette dernière solution plus générale que nous allons choisir. Soient donc $a = \sum_{i=0}^{n} a_i x^i$ et $b = \sum_{i=0}^{m} b_i x^i$ deux polynômes tels que b_m soit inversible. On notera $\mathrm{LC}(r)$ le coefficient dominant d'un polynôme r.

Algorithme 4.0.2 (Division euclidienne des polynômes)

$r = a$; $u = \mathrm{LC}(b)^{-1}$; $q = 0$
`For` i `from` $n - m$ `to` 0`:`
    `If` $\deg(r) == m + i$:
        $q = q + \mathrm{LC}(r) u x^i$; $r = r - \mathrm{LC}(r) u x^i b$
`return` (q, r)

Exemple 4.0.3 Soit $a = 3x^4 + 2x^3 + x + 5$ et $b = x^2 + 2x + 3$. On pose la division

$$
\begin{array}{rrrrrrrrrrrrr|lllll}
 & 3x^4 & + & 2x^3 & + & \cdot & + & x & + & 5 & x^2 & + & 2x & + & 3 \\
\cline{14-18}
- & (3x^4 & + & 6x^3 & + & 9x^2) & & & & & 3x^2 & - & 4x & - & 1 \\
\cline{1-10}
 & & & -4x^3 & - & 9x^2 & + & x & + & 5 & & & & & \\
 & & - & (-4x^3 & - & 8x^2 & - & 12x) & & & & & & & \\
\cline{3-12}
 & & & & & -x^2 & + & 13x & + & 5 & & & & & \\
 & & & & - & (-x^2 & - & 2x & - & 3) & & & & & \\
\cline{5-12}
 & & & & & & & 15x & + & 8 & & & & &
\end{array}
$$

pour obtenir $q = 3x^2 - 4x - 1$ et $r = 15x + 8$.

Proposition 4.0.4 Cet algorithme fournit une paire (q, r) de polynômes qui vérifient $a = bq + r$ avec $\deg(r) < \deg(b)$.

Preuve. On voit qu'à chaque étape, on a l'égalité suivante : $a = bq + r$. En effet, au départ c'est le cas : $q = 0$ et $r = a$. Ensuite, si $\deg(r) = m + i$, on a $bq + r = b(q - \mathrm{LC}(r)ux^i) + (r - \mathrm{LC}(r)ux^i b)$. Sinon, on ne change rien.

De plus, on voit que, si à un moment r est de degré supérieur ou égal à $n - m$, on va remplacer r par $r - \mathrm{LC}(r)ux^i b$ ce qui supprime le terme dominant de r et fait diminuer son degré. En fin d'algorithme, le degré de r est donc strictement inférieur à $m = \deg(b)$.

Reste à montrer l'unicité. Pour celà soient $a = bq + r = bq' + r'$ deux écritures avec $\deg(r), \deg(r') < \deg(b)$. On a $r - r' = b(q' - q)$ et donc b divise $r - r'$. Comme $\deg(r - r') < \deg(b)$ ceci n'est possible que si $r - r' = 0$ donc $r = r'$ et $q = q'$. ∎

Proposition 4.0.5 Cet algorithme utilise $(n - m + 1)(m + 2)$ multiplications et $(n - m + 1)m$ additions soit en tout $(n - m + 1)(2m + 1)$ opérations dans A.

Preuve. À chaque cycle, on multiplie $\mathrm{LC}(r)$ avec u, soit une multiplication, puis le produit $\mathrm{LC}(r)u$ avec b, soit $m + 1$ multiplications.

La soustraction correspond à additionner un polynôme avec $m + 1$ entrées et donc $m + 1$ additions. En fait, on a vu que le terme dominant de r devient nul donc on a pas besoin d'effectuer la première soustraction. Donc m additions. L'addition sur q n'ajoute qu'un monôme à un polynôme qui n'avait pas encore ce monôme, on a donc ici aucune addition.

Comme on fait $n - m + 1$ boucles, on obtient le résultat. ∎

Rapellons rapidement la division euclidienne dans le cas des entiers positifs et donnons en un algorithme. Soient donc a et b deux entiers avec $b \neq 0$.

Algorithme 4.0.6 (Division euclidienne)

$r = a$; $q = 0$
`While` $r \geq b$:
    $r = r - b$; $q = q + 1$
`return` (q, r)

Proposition 4.0.7 Cet algorithme fournit une unique paire (q, r) d'entiers positifs tels que $a = bq + r$ et $r < b$.

Preuve. À chaque étape, on a $bq + r = b(q + 1) + (r - b)$ qui reste donc constant tout au long de l'algorithme. Comme au départ, on a $q = 0$ et $r = a$, on a bien $a = bq + r$. L'algorithme se termine car r est décroissante strictement et sera donc à un moment inférieur strictement à b. L'unicité se prouve comme pour les polynômes : si on a $a = bq + r = bq' + r''$ avec $r, r' < b$, alors $r - r' = b(q - q')$. Mais on doit avoir $|r - r'| < b$ donc $r - r' = 0$ et $r = r'$ et $q = q'$. ∎

Proposition 4.0.8 Cet algorithme effectue exactement $q + 1$ additions où q est le quotient de a par b.

Preuve. À chaque étape on effectue la soustraction $r = r - b$ (donc une addition) et l'opération $q = q + 1$ qui constiste à prendre le suivant (et ne compte pas comme addition). On effectue ces opérations jusqu'à ce que q soit égal au quotient de a par b d'où le résultat. ∎

Remarque 4.0.9 Un avantage de cet algorithme est qu'il ne nécessite aucune multiplication.

5. Polynômes creux

Pour les polynômes (ou les entiers multiprécision, il peut être plus économique de représenter les polynômes d'une autre manière appelée **représentation creuse**. Cette représentation consiste à donner, pour le polynôme $a = \sum_i a_i x^i$, les paires (i, a_i) telles que $a_i \neq 0$ et seulement ces paires.

Exemple 5.0.1 Pour le polynôme $a = x^{16} + 2$, la notation "classique" consiste à donner la liste des coefficients a_i en commançant par les unités, soit ici :

$$a = (2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1).$$

La représentation creuse est beaucoup plus simple (et c'est celle que nous utilisons en écrivant $x^{16} + 2$) :

$$a = ((0, 2), (16, 1)).$$

Exemple 5.0.2 Il est à noter que c'est ainsi que sage représente la décomposition en facteurs premiers d'un entier. Il ne donne pas la liste de tous les facteurs premiers mais seulement ceux qui interviennent effectivement. Par exemple, sage revoie pour la décomposition de 242 :

$$((2, 1), (11, 2))$$

ce qui signifie que le nombre premier 2 apparaît avec multiplicité 1 alors que 11 apparaît avec multiplicité 2, soit $242 = 2 \times 11^2$. Il ne donne pas la liste de tous les premiers jusqu'à 11 :

$$242 = 2^1 \times 3^0 \times 5^0 \times 7^0 \times 11^2.$$

Définition 5.0.3 Le **poids** d'un polynôme a est

$$\omega(a) = \big|\{i \in \mathbb{N} \mid a_i \neq 0\}\big|.$$

Remarque 5.0.4 On a toujours $\omega(a) \leq \deg(a)$.

Définition 5.0.5 Un polynôme est dit **creux** si son poids est "faible" (notion à définir en fonction des besoins).

On peut montrer la proposition suivante.

Proposition 5.0.6 Il existe un algorithme permettant de multiplier des polynômes a et b en au plus $2\omega(a)\omega(b) + \omega(a) + \omega(b) + 1$ opérations

Exercice 5.0.7 Proposer un algorithme qui réalise ces bornes.

6. Puissances itérées

On a souvent besoin de calculer la puissance d'un élément a d'un anneau A c'est-à-dire a^n. Comme on l'a vu, on veut minimiser les opérations dans l'anneau, notamment les multiplications. On va dans ce chapitre donner deux algorithmes, le premier naïf et le second bien plus efficace.

Algorithme 6.0.1 (Algorithme naïf des puissances)

$b = a$
`For` i `in range` $(1, n)$`:` $b = ab$
`Return` b

Proposition 6.0.2 Cet algorithme calcule a^n et effectue $n - 1$ multiplications.

Preuve. En effet, on a $n - 1$ boucles et on multiplie b par a à chaque boucle. On a donc effectué $n - 1$ multiplications et par récurrence, on montre aisément qu'à l'étape i, la valeur de b est a^{i+1} (à l'étape 0, c'est-à-dire au départ, on a $b = a = a^1 = a^{0+1}$.∎

Voici maintenant un algorithme plus efficace qui prend en compte le fait que si on a déjà calculé une petite puissance a^m, pour obtenir rapidemant un plus grande puissance, il suffit de faire une puissance de cette puissance : $(a^m)^k = a^{km}$. C'est ce qu'on appelle une **puissance itérée**.

Pour écrire cet algorithme, il est plus pratique d'écrire n en base 2. Ce n'est pas coûteux puisque c'est ainsi que l'ordinateur stocke les données (en bits). On écrit donc n en base 2 :

$$n = n_0 + 2n_1 + \cdots + 2^r n_r = \overline{n_r \cdots n_0}^2.$$

Ici implicitement, on suppose que le premier terme de l'écriture en base 2 est non nul c'est-à-dire $n_r = 1$.

Algorithme 6.0.3 (Algorithme des puissances itérées)

$b_r = a$
`For` i `from` $r - 1$ `to` 0`:`
    `If` $n_i = 1$`:` $b_i = b_{i+1}^2 a$
    `else:` $b_i = b_{i+1}^2$
`Return` b_0

Proposition 6.0.4 Cet algorithme calcule a^n et effectue $2r = 2\log_2(n)$ multiplications.

Preuve. En effet, on a r boucles et au pire des cas, c'est-à-dire si $n_i = 1$ pour tout i, on a deux multiplications à chaque étape. On a donc $2r = 2\log_2(r)$ multiplications.

Montrons maintenant qu'on a bien calculé a^n. On montre par récurrence descendante la formule :

$$b_i = a^{n_{r-i}+2n_{r-i+1}+\cdots+2^i n_r}.$$

Pour $i = r$, on a $b_r = a = a^1 = a^{n_r}$ ce qui est ce qu'on veut. Supposons que $b_{i+1} = a^{n_{i+1}+\cdots+2^{r-i-1}n_r}$.

Si $n_i = 1$, on a $b_i = b_{i+1}^2 a = (a^{n_{i+1}+\cdots+2^{r-i-1}n_r})^2 \times a = a^{1+2n_{i+1}+\cdots+n_r\times 2^{r-i}} = a^{n_i+2n_{i+1}+\cdots+2^{r-i}n_r}$. Si $n_i = 0$, on a $b_i = b_{i+1}^2 = (a^{n_{i+1}+\cdots+2^{r-i-1}n_r})^2 = a^{0+2n_{i+1}+\cdots+2^{r-i}n_r} = a^{n_i+2n_{i+1}+\cdots+2^{r-i}n_r}$. Ce qui prouve la formule. Pour b_0, on obtient donc

$$b_0 = a^{n_0+2n_1+\cdots+2^r n_r} = a^n,$$

ce qui termine la preuve. ∎

Deuxième partie .

Anneaux euclidiens, principaux et factoriels

Nous étudions les anneaux dans lesquels il existe une décomposition unique en produits d'éléments indécomposables. Les modèles de tels anneaux sont les anneaux $\mathbb{Z}$ et l'anneau de polynômes sur un corps.

7. Anneaux intègres, euclidiens et principaux

7.1. Anneaux intègres

Définition 7.1.1 Un anneau A est dit **intègre** si pour $a, b \in A$, on a l'implication $(ab = 0 \Rightarrow a = 0 \text{ ou } b = 0)$.

Exemple 7.1.2 L'anneaux $\mathbb{Z}$ est intègre.

Exemple 7.1.3 Un corps est un anneau intègre.

Exemple 7.1.4 L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre. En effet, on a $[2] \neq 0$ et $[3] \neq 0$ mais $[2][3] = [6] = 0$.

Proposition 7.1.5 Si A est un anneau intègre, alors $A[x]$ est un anneau intègre.

Preuve. Soient $a, b \in A[x]$ tels que $ab = 0$. Supposons que a et b sont non nuls. Alors, on peut écrire $a = a_0 + \cdots + a_n x^n$ avec $a_n \neq 0$ et $b = b_0 + \cdots + b_m x^m$ avec $b_m \neq 0$. On a alors $ab = c = c_0 + \cdots + c_{n+m} x^{n+m}$. Nous ne chercherons pas à calculer tous les coefficients de c mais son coefficient dominant est $c_{n+m} = a_n b_m$. Comme $c = ab = 0$, on doit avoir $a_n b_m = c_{n+m} = 0$. Ce qui impose, comme A est intègre, que $a_n = 0$ ou $b_m = 0$. Une contradiction. ∎

Corollaire 7.1.6 L'anneau $\mathsf{k}[x]$ avec k un corps est un anneau intègre.

Définition 7.1.7 Soit A un anneau. Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que $ab = 1$. L'ensemble des éléments inversibles est noté $A^\times$.

Exemple 7.1.8 On a $\mathbb{Z}^\times = \{1; -1\}$.

Exercice 7.1.9 Soit k un corps. Montrer que $\mathsf{k}[x]^\times = \mathsf{k} \backslash \{0\}$ l'ensemble des polynômes constants non nuls.

Lemme 7.1.10 Soit a inversible, l'élément b tel que $ab = 1$ est unique. □

Preuve. Exercice. ∎

Définition 7.1.11 Soit A un anneau, a un élément inversible. L'élément b tel que $ab = 1$ est appelé **inverse** de a et est noté a^{-1}.

7.2. Anneaux euclidiens

Définition 7.2.1 Un anneau **euclidien** est un anneau intègre muni d'une fonction $d : A \setminus \{0\} \to \mathbb{N}$ (appelée **stathme**) telle que pour tout $a \in A$ et tout $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que

1. $a = bq + r$ et
2. $r = 0$ ou $d(r) < d(b)$.

Exemple 7.2.2 L'anneau $\mathbb{Z}$ des entiers muni du stathme $d(a) = |a|$ est un anneau euclidien.

Exemple 7.2.3 Soit k un corps, l'anneau $\mathsf{k}[x]$ de polynômes à coefficients dans k muni du stathme $d(a) = \deg(a)$ est un anneau euclidien.

7.3. Anneaux principaux

Définition 7.3.1 Soit A un anneau. Un sous-ensemble I de A est appelé **idéal** si les deux conditions suivantes sont satisfaites :

1. I est un sous-groupe de A pour l'addition et
2. pour tout $a \in I$ et tout $b \in A$, on a $ab \in I$.

Lemme 7.3.2 Soit I un idéal de A. La relation suivante est une relation déquivalence :

$$a \sim b \Leftrightarrow a - b \in I.$$

On note A/I l'ensemble des classes pour cette relation d'équivalence et on note $[a]$ la classe de a. On note $p : A \to A/I$ l'application définie par $p(a) = [a]$. C'est la projection canonique de A sur A/I. □

Preuve. Exercice. ■

Lemme 7.3.3 Soit I un idéal de A. L'ensemble A/I est muni d'une structure d'anneau définie par

$$[a] + [b] = [a + b] \text{ et } [a][b] = [ab].$$

De plus, pour cette structure d'anneau, la projection canonique est un morphisme d'anneau. □

Preuve. Exercice. ■

Exemple 7.3.4 Dans $\mathbb{Z}$ les idéaux sont tous de la forme $n\mathbb{Z} = \{\text{multiples de } n\}$. Le quotient est l'anneau bien connu des entiers modulo n, noté $\mathbb{Z}/n\mathbb{Z}$.

La projection canonique $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est le passage modulo n.

Définition 7.3.5 Soit A un anneau et $a \in A$. **L'idéal engendré** par a est l'ensemble

$$(a) = \{ab \in A \mid b \in A\}.$$

Exemple 7.3.6 Dans $\mathbb{Z}$, on a $n\mathbb{Z} = (n)$: l'idéal $n\mathbb{Z}$ est l'idéal engendré par n.

Exemple 7.3.7 Dans un anneau quelconque, on a toujours les idéaux (0) et (1).

L'idéal nul (0) ne contient que l'élément 0 : $(0) = \{0\}$. L'idéal (1) est l'aneau tout entier : $(1) = A$.

Définition 7.3.8 Soit A un anneau et $a_1, \cdots, a_n \in A$. **L'idéal engendré** par $a_1, \cdots, a_n$ est l'ensemble

$$(a_1, \cdots, a_n) = \{a_1b_1 + \cdots + a_nb_n \in A \mid b_1, \cdots, b_n \in A\}.$$

Exemple 7.3.9 Dans $\mathbb{Z}$, on peut regarder l'idéal

$$I = (6, 9) = \{6i + 9j \in \mathbb{Z} \mid i, j \in \mathbb{Z}\}.$$

Exercice 7.3.10 Montrer que l'on a $(6, 9) = (3)$.

Définition 7.3.11 Soit A un anneau.

1. Un idéal I de A est dit **principal** s'il existe un élément $a \in A$ tel que $I = (a)$.

2. Un anneau A est dit principal si A est intègre et tous ses idéaux sont principaux.

Théorème 7.3.12 Un anneau euclidien est toujours principal. □

Preuve. Soit A un anneau euclidien. Soit I un idéal, il faut montrer qu'il existe a tel que $I = (a)$. Si $I = (0)$, on a fini. Sinon, on pose

$$n = \min\{d(a) \mid a \in I \text{ et } a \neq 0\}.$$

Soit b tel que $b \in I$, $b \neq 0$ et $d(b) = n$. On va montrer que $I = (b)$.

Si $a \in (b)$, alors il existe $c \in A$ tel que $a = bc$. Comme $b \in I$ ceci impose que $a \in I$.

Réciproquement, soit $a \in I$. On sait qu'il existe $q, r \in A$ avec $r = 0$ ou $d(r) < d(b)$ tels que $a = bq + r$. On voit alors que $r = a - bq$ et comme $a, b \in I$, on a aussi $r \in I$. Si $r \neq 0$, on a $d(r) < d(b) = n$ etce qui contredit la minimalité de n. On a donc $r = 0$ et $a = bq$ c'est-à-dire $a \in (b)$. ■

Corollaire 7.3.13 Les anneaux $\mathbb{Z}$ et $\mathsf{k}[x]$ sont principaux.

Exemple 7.3.14 Dans $\mathbb{Z}$, on a $(6, 9) = (3)$.

Proposition 7.3.15 Soit A un anneau intègre et $a, b \in A$. Si $(a) = (b)$, alors il existe un élément $u \in A^\times$ tel que $b = ua$.

Preuve. Si $a = 0$, alors $\{0\} = (0) = (a) = (b)$ et donc $b = 0 = a$ et on peut prendre $u = 1$.

On peut donc supposer $a \neq 0$. Comme $b \in (b) = (a)$, il existe $u \in A$ tel que $b = ua$. De même, comme $a \in (a) = (b)$, il existe $v \in A$ tel que $a = vb$. On obtient $a = vb = vua$. On obtient $a(1 - uv) = 0$. Comme $a \neq 0$, ceci impose (A intègre) que $1 - uv = 0$ donc $uv = 1$ et u est inversible d'inverse v. On a gagné. ∎

Exemple 7.3.16 Dans $\mathbb{Z}$, si $n\mathbb{Z} = m\mathbb{Z}$, alors $m = \pm n$.

8. pgcd, ppcm et algorithme d'Euclide

8.1. pgcd et ppcm

Lemme 8.1.1 Soit A un anneau et I et J deux idéaux. Alors les ensembles suivants sont des idéaux :

1. L'intersection $I \cap J$ et
2. La somme $I + J = \{a + b \in A \mid a \in I \text{ et } b \in J\}$. □

Preuve. Exercice. ■

Lemme 8.1.2 Soit A un anneau et $a, b \in A$. Alors on a $(a) + (b) = (a, b)$. □

Preuve. Exercice. ■

Définition 8.1.3 Soit A un anneau principal et soient $a, b \in A$.

1. Un **pgcd ou plus grand commun diviseur** de a et b est un élément $\text{pgcd}(a, b)$ tel que $(a) + (b) = (a, b) = (\text{pgcd}(a, b))$.

2. Un **ppcm ou plus petit commun multiple** de a et b est un élément $\text{ppcm}(a, b)$ tel que $(a) \cap (b) = (\text{ppcm}(a, b))$.

Exemple 8.1.4 Dans $\mathbb{Z}$, on a $(6) + (9) = (6, 9) = (3) = (\text{pgcd}(6, 9))$ et $(6) \cap (9) = (18) = (\text{ppcm}(6, 9))$.

Remarque 8.1.5 Les pgcd et les ppcm sont uniques à mutiplication par un inversible près. Dans $\mathbb{Z}$ par exemple, on a que 3 et -3 sont des pgcd de 6 et 9.

Proposition 8.1.6 Soit A u anneau et $a, b \in A$.

1. Un $\text{pgcd}(a, b)$ de a et b est un plus grand commun diviseur au sens suivant : si d divise a et b, alors d divise $\text{pgcd}(a, b)$.

2. Un $\text{ppcm}(a, b)$ de a et b est un plus petit commun multiple au sens suivant : si m est un multiple a et b, alors m est un multiple de $\text{ppcm}(a, b)$.

Preuve. 1. Soit d un diviseur de a et b. On a $\text{pgcd}(a,b) = (a,b)$ donc il existe $u, v \in A$ tels que $\text{pgcd}(a,b) = au + bv$. Comme d divise a et b, il doit diviser leur somme.

2. Soit m un multiple de a et b. Il existe donc $u, v \in A$ tels que $m = ua$ et $m = vb$. On obtient $m \in (a)$ et $m \in (b)$ donc $m \in (a) \cap (b) = (\text{ppcm}(a,b))$ donc $\text{ppcm}(a,b)$ divise m. ∎

8.2. Algorithme d'Euclide

Pour les anneaux euclidiens, il existe une technique effective pour trouver le pgcd. Soit A un anneau euclidien.

Proposition 8.2.1 Soient $a, b \in A$ et soient q et r tels que $a = bq + r$. Alors, à un inversible près, on a

$$\text{pgcd}(a,b) = \text{pgcd}(r,b).$$

Preuve. Il suffit de montrer que $(\text{pgcd}(a,b)) = (a,b) = (r,b) = (\text{pgcd}(r,b))$. On a bien sûr $b \in (r,b)$ et $a = bq + r \in (r,b)$. On obtient $(a,b) \subset (r,b)$. Réciproquement, on a $b \in (a,b)$ et $r = a - bq \in (a,b)$ donc $(r,b) \subset (a,b)$ et le résultat en découle. ∎

Dans l'algorithme suivant, on écrira $a\%b$ pour le reste de a par b dans la division euclidienne.

Algorithme 8.2.2 (Algorithme d'Euclide)

$r_0 = a$; $r_1 = b$
$i = 1$
`While` $r_i \neq 0$:
    $r_{i+1} = r_{i-1}\%r_i$; $i = i + 1$
`Return` r_{i-1}

Proposition 8.2.3 L'algorithme d'Euclide fournit le pgcd de a et de b.

Preuve. On commence par montrer que $\text{pgcd}(r_i, r_{i+1}) = \text{pgcd}(a,b)$ pour tout $i \geq 0$. En effet, on a $\text{pgcd}(r_{i+1}, r_i) = \text{pgcd}(r_i\%r_{i-1}, r_i) = \text{pgcd}(r_{i-1}, r_i)$. Par récurrence, on obtient $\text{pgcd}(r_i, r_{i+1}) = \text{pgcd}(r_0, r_1) = \text{pgcd}(a,b)$.

Lorsque l'algorithme s'arrête, on a $r_{i-2}\%r_{i-1} = r_i = 0$ et donc r_{i-1} divise r_{i-2}. On en déduit $\text{pgcd}(a,b) = \text{pgcd}(r_{i-2}, r_{i-1}) = r_{i-1}$.

On vérifie enfin que l'algorithme s'arrête. En effet, pour $i \geq 1$, on a $d(r_{i+1}) < d(r_i)$ donc la suite des $d((r_i))_{i\geq 1}$ est strictement décroissante. Comme c'est une suite d'entiers, elle ne peut être infinie. ∎

Proposition 8.2.4 Dans l'anneau des polynômes $\mathsf{k}[x]$, et pour a de degré n et b de degré m, l'algorithme d'Euclide simple effectue $2nm + n + m + 1$ opérations dans k.

Preuve. Soit l la valeur de i à la fin de l'algorithme. À chaque étape, on effectue la division euclidienne de r_{i-1} par r_i. Cette division euclidienne nécessite $(2n_i+1)(n_{i-1}-n_i+1)$ opérations où $n_i = \deg(r_i)$. On a donc effectué

$$\sum_{i=1}^{l}(2n_i+1)(n_{i-1}-n_i+1)$$

opérations. Au pire à chaque étape, le degré de r_i diminue de 1. On a donc $n_0 = n$, $n_1 = m$ et au pire $n_i = \deg(r_i) = m+1-i$ pour $i \in [2,l]$ et $l = m+1$. On obtient

$$\begin{aligned}\sum_{i=1}^{l}(2n_i+1)(n_{i-1}-n_i+1) &= (2m+1)(n-m+1)+\sum_{i=2}^{m+1}(2(m+1-i)+1)2\\ &= (2m+1)(n-m+1)+\sum_{i=0}^{m-1}(4i+2)\\ &= 2nm+n+m+1.\end{aligned}$$

Proposition 8.2.5 Soient A un anneau et $a, b \in A$. Alors il existe, $u, v \in A$ tels que

$$\mathrm{pgcd}(a,b) = au+bv.$$

Preuve. En effet, $\mathrm{pgcd}(a,b) \in (a)+(b) = (a,b)$. ∎

L'algorithme d'Euclide étendu fourni à la fois le pgcd et les éléments u, v tels que $\mathrm{pgcd}(a,b) = au+bv$. Dans l'algorithme suivant, on écrira $a//b$ pour le quotient de a par b dans la division euclidienne.

Algorithme 8.2.6 (Algorithme d'Euclide étendu)

$r_0 = a$; $r_1 = b$
$s_0 = 1$; $s_1 = 0$
$t_0 = 0$; $t_1 = 1$
$i = 1$
`While` $r_i \neq 0$:
    $q_i = r_{i-1}//r_i$
    $r_{i+1} = r_{i-1} - q_i r_i$
    $s_{i+1} = s_{i-1} - q_i s_i$
    $t_{i+1} = t_{i-1} - q_i t_i$
    $i = i+1$
$l = i-1$
`return` l
`return` (r_i, s_i, t_i) `for i in range (0,l+2)`
`return` q_i `for i in range (1,l+1)`

Proposition 8.2.7 Avec les notations de l'algorithme d'Euclide étendu, on a

1. $s_i a + t_i b = r_i$ pour tout $i \in [0, l+1]$;
2. $\text{pgcd}(a,b) = \text{pgcd}(r_i, r_{i+1}) = r_l$ pour tout i.

En particulier, l'algorithme d'Euclide étendu nous fournit la solution (s_l, t_l) de l'équation $au + bv = \text{pgcd}(a,b)$.

Preuve. 1. On procède par récurrence sur i. Pour $i = 0$ et $i = 1$, on a $s_0 a + t_0 b = a = r_0$ et $s_1 a + t_1 b = b = r_1$. Supposons maintenant que l'on a $s_i a + t_i b = r_i$ et $s_{i-1} a + t_{i-1} b = r_{i-1}$. On obtient

$$s_{i+1}a+t_{i+1}b = (s_{i_1}-q_i s_i)a+(t_{i-1}-q_i t_i)b = (s_{i-1}a+t_{i-1}b)-q_i(s_{i-1}a+t_{i-1}b) = r_{i-1}-q_i r_i$$

et comme $r_{i+1} = r_{i-1} - q_i r_i$, on en déduit $s_{i+1} a + t_{i+1} b = r_{i+1}$.

2. On montre par récurrence que $\text{pgcd}(r_{i-1}, r_i) = \text{pgcd}(r_i, r_{i+1})$. En effet, on a $q_i = r_{i-1} // r_i$ et $r_{i+1} = r_{i-1} - q_i r_i$. Ceci impose que l'écriture $r_{i-1} = r_i q_i + r_{i+1}$ est la division euclidienne de r_{i-1} par r_i. On en déduit que r_{i+1} est le reste de cette division et donc qu'on a l'égalité $\text{pgcd}(r_{i-1}, r_i) = \text{pgcd}(r_i, r_{i+1})$.

Le $\text{pgcd}(r_i, r_{i+1})$ est donc indépendant de i. Pour $i = 0$, on obtient $\text{pgcd}(a,b)$. Pour $i = l$, on a $r_{l+1} = 0$ donc $\text{pgcd}(r_l, r_{l+1}) = \text{pgcd}(r_l, 0) = r_l$.

La dernière assertion découle de l'égalité 1. appliquée à $i = l$. On obtient grâce à 2. :

$$s_l a + t_l b = \text{pgcd}(r_l, r_{l+1}) = r_l = \text{pgcd}(a,b).$$

Remarque 8.2.8 On peut demander à l'algorithme étendu de ne renvoyer que les triplets $(u, v, \text{pgcd}(a,b))$ solutions de $au + bv = \text{pgcd}(a,b)$. Pour celà il suffit de lui de mander de renvoyer (s_l, t_l, r_l).

Les résultats intermédiaires peuvent servir dans d'autres algorithmes dont nous ne parlerons pas dans ce cours.

Proposition 8.2.9 Dans l'anneau des polynômes $\mathsf{k}[x]$, et pour a de degré n et b de degré m, l'algorithme d'Euclide étendu effectue $6nm + O(n)$ opérations dans k.

Exercice 8.2.10 Vérifier la complexité donnée dans l'algorithme précédent. On pourra d'abord montrer les formules suivantes :

$$\deg(s_i) = \sum_{j=2}^{i-1} \deg(q_j) \text{ et } \deg(t_i) = \sum_{j=1}^{i-1} \deg(q_j).$$

Proposition 8.2.11 Dans $\mathbb{Z}$, et pour a de longueur n et b de longueur m, l'algorithme d'Euclide étendu effectue $O(nm)$ opérations processeurs.