Factorisation dans $\mathbb{Z}[X]$

Une caractérisation des irréductibles de $\mathbb{Z}[X]$
Implémentation en OCaml avec une complexité en temps polynomiale

Nicolas Kress

2024-2025

Table des matières

1 Motivation

Le problème de la factorisation d'un polynôme est loin d'être un problème récent : on trouve des débuts chez Diophante au IIe siècle, puis chez Viète, comme chez Descartes, avant que beaucoup d'autres ne s'y intéressent. Factoriser permet de mettre en évidence les racines d'un polynôme, et de le manipuler plus facilement. L'un des plus grands problèmes est l'identification des irréductibles d'un anneau des polynômes.
On possède une caractérisation des irréductibles de $\mathbb{R}[X]$ à l'aide du discriminant : ceci s'étend mal à $\mathbb{Q}[X]$ ou à $\mathbb{Z}[X]$.

Pour remédier à ce fait, Eisenstein publie [2] en 1850 le critère qui porte aujourd'hui son nom, apportant une condition suffisante pour qu'un polynôme à coefficients entiers soit irréductible. Ce n'est cependant toujours pas satisfaisant à la résolution pratique du problème. En 1967, Elwyn Berlekamp démontre un algorithme de factorisation de polynômes sur les corps finis $\mathbb{F}_p$ [3], permettant alors de factoriser modulo un nombre premier p. Il suffit alors de remonter cette factorisation, ce qui se fait par le lemme de Hensel. Le lemme de Hensel [4], démontré au début du XXe siècle, permet d'approcher des racines modulo p dans l'anneau des entiers p-adiques. Une fois ce lemme adapté, ce qui a été fait à la fin du XXe siècle, on peut remonter une factorisation modulo p^k à une factorisation modulo p^{k+1}.

L'objet de ce travail est de fournir une réunion de ces résultats. Ceci a déjà été fait maintes fois, tel par exemple par Roland Abuaf et Ivan Boyer en 2007 [1]. La factorisation dans $\mathbb{Z}[X]$ est en outre souvent un sujet enseigné en deuxième année de Master [5]. L'objectif cette fois-ci est d'illustrer les propos, de les justifier complètement, notamment avec une implémentation complète en OCaml. En détaillant les complexités, nous monterons par ailleurs que le problème de la factorisation dans $\mathbb{Z}[X]$ se résout en temps polynomial (dont la définition sera explicitée à la partie 8.1). Au contraire de certaines autres

publications, nous relierons les résultats établis ici à d'autres résultats connus, tel, par exemple, le critère d'Eisenstein.

2 Définitions formelles et réduction préliminaire

2.1 Irréductibilité, contenu, et polynômes primitifs sur $\mathbb{Z}$

Définition 2.1. *Soit* $\mathbf{A}$ *un anneau commutatif. Soit* $\mathbf{B}$ *un sous-anneau de* $\mathbf{A}$*. On note* $\mathbf{A}[X]$ *l'anneau de polynômes à coefficients dans* $\mathbf{A}$*. On dit que* $P \in \mathbf{B}[X]$ *est* ***irréductible*** *sur* $\mathbf{A}[X]$ *s'il est non nul, non inversible dans* $\mathbf{A}[X]$ *et si pour tous* $Q, R \in \mathbf{A}[X]$ *tels que* $P = QR$*, alors soit* Q *soit* R *est inversible.*

Définition 2.2 (Contenu et polynôme primitif)**.** *Soit* $P \in \mathbb{Z}[X]$*. On appelle* ***contenu*** *de* P *le plus grand diviseur commun (pgcd) de ses coefficients.*
On dira que P *est* ***primitif*** *lorsque* $C(P) = 1$*. Un polynôme unitaire est primitif.*

Lemme 2.1 (Lemme de Gauss)**.** *Le produit de deux polynômes primitifs est primitif et le contenu* C *est multiplicatif :*

$$\forall P, Q \in \mathbb{Z}[X], \quad C(PQ) = C(P)C(Q)$$

Démonstration. Cette démonstration s'inspire de la démonstration de la source [4]. Soient $P = \sum_{k=0}^{p} a_k X^k, Q = \sum_{k=0}^{q} b_k X^k \in \mathbb{Z}[X]$ non nuls. On raisonne par induction sur $p+q$. Quitte à diviser par $C(P)$ et $C(Q)$ respectivement, on peut supposer P, Q primitifs. On pose :

$$c := C(PQ), \quad d := \text{pgcd}(c, a_p)$$

Alors

$$\frac{(P - a_p X^p)Q}{d} \in \mathbb{Z}[X]$$

Si $P = a_p X^p$, alors le résultat est immédiat (car $C(P) = a_p$, et $C(PQ) = C(a_p X^p Q) = a_p C(X^p Q) = C(P)C(Q)$). Sinon, on a par induction que $d | C(P - a_p X^p)C(Q)$. Comme Q est primitif, on a $d | C(P - a_p X^p)$. Donc $d | C(P)$. Dès lors, P étant primitif, $d = \text{pgcd}(c, a_p) = 1$. On montre de même $\text{pgcd}(c, b_q) = 1$. On en déduit alors $c = \text{pgcd}(c, a_p b_q) = 1$, et PQ est primitif. Dans le cas où P, Q ne sont pas primitifs, on a :

$$C(PQ) = C(P)C(Q)C(\frac{P}{C(P)}\frac{Q}{C(Q)}) = C(P)C(Q)$$

Car le produit $\frac{P}{C(P)}\frac{Q}{C(Q)}$ est primitif par ce qui précède. □

Lemme 2.2. *Si* $P \in \mathbb{Z}[X]$ *est primitif et irréductible sur* $\mathbb{Q}[X]$*, alors il est irréductible sur* $\mathbb{Z}[X]$*.*

Démonstration. Si P est primitif et n'est pas irréductible sur $\mathbb{Z}[X]$, alors on peut écrire $P = QR$ où $Q, R \in \mathbb{Z}[X]$ sont non inversibles. Or, par le lemme de Gauss précédent, $C(P) = C(Q)C(R) = 1$, donc Q et R sont primitifs. On en déduit que $\deg Q, \deg R \geq 1$, donc Q, R ne sont pas inversibles dans $\mathbb{Q}[X]$. Donc P n'est pas irréductible dans $\mathbb{Q}[X]$. □

Remarque 2.1. L'hypothèse « P est primitif » est essentielle. Le polynôme $2X$ est irréductible sur $\mathbb{Q}[X]$, mais pas sur $\mathbb{Z}[X]$, car $2X = 2 \times X$, où 2 et X sont non inversibles dans $\mathbb{Z}$.

Lemme 2.3. *Le problème d'irréductibilité* ***d'un polynôme primitif*** *sur* $\mathbb{Q}[X]$ *est le même que sur* $\mathbb{Z}[X]$.

Démonstration. Soit $P \in \mathbb{Z}[X]$ primitif. S'il est irréductible sur $\mathbb{Q}[X]$, alors il est irréductible sur $\mathbb{Z}[X]$ par le lemme précédent.

Réciproquement, si P n'est pas irréductible sur $\mathbb{Q}[X]$, on note $P = QR$ avec $Q, R \in \mathbb{Q}[X]$. On note q (resp. r) le plus petit multiple commun (ppcm) des dénominateurs des coefficients de Q (resp. R). Alors $qQ, rR \in \mathbb{Z}[X]$, et

$$C(qQrR) = C(qQ)C(rR)$$

par le lemme de Gauss. Dès lors,

$$qr = qrC(P) = C(qrP) = C(qQrR) = C(qQ)C(rR)$$

ou encore :

$$P = \frac{qQ}{C(qQ)} \frac{rR}{C(rR)}$$

donc P n'est pas irréductible sur $\mathbb{Z}[X]$. □

Remarque 2.2. Si $P \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}[X]$, alors ou bien P est de valeur constante un nombre premier, ou bien $|C(P)| = 1$. En effet, si on suppose $|C(P)| \neq 1$ et $\deg P \geq 1$, on peut prendre $C(P)$ comme facteur non inversible dans $\mathbb{Z}[X]$ de P.

Définition 2.3. *On dit que* $P \in \mathbf{A}[X]$ *est* ***sans facteurs carrés*** *lorsque la décomposition en facteurs irréductibles de* P *n'admet pas de facteurs carrés ; i.e*

$$\forall f_1, ...f_r \text{ irreductibles}, \ \forall a_1, ..., a_r \in \mathbb{N}, \quad P = f_1^{a_1}...f_r^{a_r} \implies a_1, ...a_r \leq 1$$

Lemme 2.4. *On peut toujours se ramener à l'étude d'un polynôme de* $\mathbb{Z}[X]$ *unitaire et sans facteurs carrés.*

Démonstration. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ non nul. Si P n'est pas sans facteurs carrés, alors $\text{pgcd}(P, P')$ est déjà un facteur non-trivial de P. Si P n'est pas unitaire, on remarque que :

$$P(X) = \sum_{k=0}^{n} a_k X^k = \frac{1}{a_n^{n-1}}[(a_n X)^n + \sum_{k=0}^{n-1} a_k a_n^{n-1-k}(a_n X)^k] := \frac{1}{a_n^{n-1}} \hat{P}(a_n X)$$

Le polynôme $\hat{P}$ défini ci-dessus sera par la suite appelé le **réduit** du polynôme P. Le polynôme $\hat{P} \in \mathbb{Z}[X]$ ainsi défini est alors unitaire. Factoriser $\hat{P}$ revient alors à factoriser P. Soit $Q \in \mathbb{Q}[X]$ non nul. Soit q le plus petit multiple commun des dénominateurs des coefficients de Q. Soit $R \in \mathbb{Z}[X]$ unitaire et sans facteurs carrés associé à qQ par ce qui précède. Alors

$$Q = \frac{1}{q\alpha^{n-1}} R$$

où $n := \deg Q$ et α est le coefficient dominant de Q. Alors Q est irréductible dans $\mathbb{Q}[X]$ si et seulement si R est irréductible dans $\mathbb{Q}[X]$ c'est-à-dire si et seulement si R est irréductible dans $\mathbb{Z}[X]$ par application du lemme 2.3, puisque R est unitaire (donc primitif). □

Lemme 2.5. *L'irréductibilité sur $\mathbb{Q}[X]$ de polynômes à coefficients entiers est invariante par $f \mapsto \hat{f}$.*

Démonstration. En guise d'illustration, commençons par traiter le cas $P = aX + b \in \mathbb{Z}[X]$, où $a \neq 0$. Alors $\hat{P} = X + b$. P et $\hat{P}$ sont alors irréductibles sur $\mathbb{Q}[X]$. Remarquons cependant que ce n'est pas le cas sur $\mathbb{Z}[X]$, puisqu'il suffit que $\text{pgcd}(a, b) \neq 1$. On ne peut donc que montrer l'invariance de l'irréductibilité sur $\mathbb{Q}[X]$. Revenons au cas général. Soit $f \in \mathbb{Z}[X]$. On suppose f irréductible sur $\mathbb{Q}[X]$. Alors, si $\hat{f} = gh$, où $g, h \in \mathbb{Q}[X]$, on a

$$f = \frac{1}{a_n^{n-1}} g(a_n X) h(a_n X) \tag{1}$$

ce qui implique g ou h constant. Donc $\hat{f}$ est irréductible sur $\mathbb{Q}[X]$. Notamment, par le lemme 2.3, $\hat{f}$ est irréductible sur $\mathbb{Z}[X]$.

Réciproquement, supposons f non irréductible sur $\mathbb{Q}[X]$ et notons $f = gh$, avec $g, h \in \mathbb{Q}[X]$ non inversibles (i.e non constants). On a alors

$$\hat{f} = \frac{1}{a_n} \times a_n^{\deg g} g(\frac{X}{a_n}) \times a_n^{\deg h} h(\frac{X}{a_n}) \tag{2}$$

Donc $\hat{f}$ n'est pas irréductible dans $\mathbb{Q}[X]$. □

2.2 Résultats sur le résultant

Définition 2.4 (Matrice de Sylvester)**.** *Soit* $\mathbf{A}$ *un anneau commutatif. Soient* $P = \sum_{k=0}^{p} a_k X^k$, $Q = \sum_{j=0}^{q} b_k X^k \in \mathbf{A}[X]$. *On appelle* ***Matrice de Sylvester*** *associée à P et Q la matrice carrée de taille $(p+q)$:*

$$\begin{pmatrix}
a_p & 0 & - & 0 & b_q & 0 & - & 0 \\
a_{p-1} & a_p & - & 0 & b_{q-1} & b_q & - & 0 \\
a_{p-2} & a_{p-1} & - & 0 & b_{q-2} & b_{q-1} & - & 0 \\
| & | & & | & | & | & & 0 \\
a_0 & a_1 & - & a_p & b_1 & b_2 & - & b_q \\
0 & a_0 & - & a_{p-1} & b_0 & b_1 & - & b_{q-1} \\
| & | & & | & | & | & & | \\
0 & 0 & - & a_0 & 0 & 0 & - & b_0
\end{pmatrix}$$

où les m premières colonnes dépendent de P, et les n dernières colonnes dépendent de Q.

Définition 2.5 (Résultant, discriminant)**.** *Soit $\mathbf{A}$ un anneau commutatif. Soient $P = \sum_{k=0}^{p} a_k X^k,\ Q = \sum_{j=0}^{q} b_k X^k \in \mathbf{A}[X]$. On appelle **résultant** de P, Q, et on notera $\mathrm{Res}(P, Q)$ le déterminant de la Matrice de Sylvester associée à P et Q. Lorsque $Q = P'$, on appellera **discriminant** de P l'élément de $\mathbf{A}$:*

$$\Delta(P) := \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n}\mathrm{Res}(P, P')$$

Exemple. Si $P = aX^2 + bX + c$, avec $a \neq 0$, alors la matrice de Sylvester prend la forme :

$$\begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix}$$

de déterminant $ab^2 + 4a^2c - 2ab^2$, d'où la formule bien connue du discriminant pour un polynôme de degré 2 :

$$\Delta(aX^2 + bX + c) \quad = -\frac{4a^2c - ab^2}{a} = b^2 - 4ac$$

Lemme 2.6 (Propriétés du résultant)**.** *Soient $P, Q \in \mathbf{A}[X]$. On suppose $m := \deg Q > 0$. Soit $\alpha \in \mathbf{A}$. Alors :*

1. $\mathrm{Res}(\alpha, Q) = \alpha^m$
2. $\mathrm{Res}(Q, Q) = 0$
3. $\mathrm{Res}(\alpha P, Q) = \alpha^m \mathrm{Res}(P, Q)$
4. $\mathrm{Res}(P, Q) = (-1)^{m \times \deg P}\mathrm{Res}(Q, P)$

Démonstration.

1. Immédiat par les propriétés du déterminant.
2. Les colonnes de la matrice de Sylvester sont liées.
3. Les m premières colonnes ont été multipliées par α. On conclut par les propriétés multiplicatives du déterminant.
4. On échange successivement des colonnes de la matrice de Sylvester jusqu'à obtenir la matrice de Sylvester associée à Q et à P. On effectue au total nm échanges, où $n = \deg P$.

□

Remarque 2.3. Avant de poursuivre, faisons les remarques suivantes :

1. $\mathrm{Res}(P, Q)$ est un élément de $\mathbf{A}$. On l'identifiera à un polynôme de $\mathbf{A}_1[X]$.
2. La matrice de Sylvester est la matrice de la famille

   $$(X^{q-1}P, ..., XP, P, X^{p-1}Q, ..., XQ, Q)$$

   dans la base $(X^{p+q-1}, ..., X, 1)$.

3. On trouvera dans la littérature que la matrice de Sylvester est définie comme la transposée de la matrice ci-dessus. On introduit cette écriture afin de s'éviter le passage par les transposées dans ce qui suit. Le déterminant de Sylvester (c'est-à-dire le résultant), qui est le point le plus important dans le cadre des résultats suivants, n'est pas changé par cette définition.

Théorème 2.1. *Il existe* $U, V \in \mathbf{A}[X]$ *tels que* $\deg U < p$, $\deg V < q$, *et :*

$$UP + VQ = \mathrm{Res}(P, Q)$$

Démonstration. Posons l'application linéaire

$$\begin{array}{rcl} \phi_{P,Q} & : & \mathbf{A}_{q-1}[X] \times \mathbf{A}_{p-1}[X] \to \mathbf{A}_{p+q-1}[X] \\ & & (U, V) \mapsto UP + VQ \end{array}$$

Alors la matrice de $\phi_{P,Q}$ dans la base $((X^{q-i}, 0)_{1 \leq i \leq q}, (0, X^{p-j})_{1 \leq j \leq p})$ de départ et dans la base $(X^{p+q-1}, ..., X, 1)$ à l'arrivée est la matrice de Sylvester associée à P, Q (voir remarque 2.3). Dès lors, le déterminant de $\phi_{P,Q}$ dans ces bases est $\mathrm{Res}(P, Q)$. Notons de plus ψ l'application linéaire associée à la transposée de la comatrice de $\phi_{P,Q}$. On a alors

$$\phi_{P,Q} \circ \psi \quad = \quad \mathrm{Res}(P, Q)\mathrm{Id}$$

Dès lors, en évaluant en 1, et en posant $(U, V) := \psi(1) \in \mathbf{A}_{q-1}[X] \times \mathbf{A}_{p-1}[X]$, on a

$$UP + VQ \quad = \quad \mathrm{Res}(P, Q)$$

□

Lemme 2.7. *Si* $\mathbf{A}$ *est factoriel, alors pour tous* $P, Q \in \mathbf{A}[X]$,

$$\mathrm{Res}(P, Q) = 0 \quad \Longleftrightarrow \quad P, Q \textit{ admettent un diviseur commun non constant}$$

Démonstration. On suppose P, Q tous deux non nuls. On note $p := \deg P$, $q := \deg Q$. Supposons le résultant $\mathrm{Res}(P, Q)$ nul. Alors $\phi_{P,Q}$ (introduit à la démonstration de 2.1) n'est pas injective : il existe un couple $(U, V) \in \mathbf{A}_{q-1}[X] \times \mathbf{A}_{p-1}[X]$ non nul tels que

$$UP + VQ = 0$$

Dès lors,

$$UP = -VQ$$

Comme $\mathbf{A}$ est supposé factoriel, $\mathbf{A}[X]$ l'est aussi. Notons $P_1, ...P_r$ les facteurs irréductibles de P dans $\mathbf{A}[X]$. Si aucun P_i ne divise Q, alors ils divisent tous V : ceci implique alors $\deg V > \deg P_1 + ... + \deg P_r = \deg P$, (car $V \neq 0$), ce qui est absurde. Donc il existe $i_0 \in \{1, ..., r\}$ tel que P_{i_0} divise Q. Or P_{i_0} est irréductible, donc non inversible dans $\mathbf{A}[X]$, d'où :

$$P_{i_0} \text{ est un facteur non trivial de } P \text{ et de } Q$$

Réciproquement, supposons disposer de $\Delta \in \mathbf{A}[X]$ non constant tel que $P = \overline{P}\Delta$ et $Q = \overline{Q}\Delta$. Par le théorème précédent (2.1), il existe $(U, V) \in \mathbf{A}_{q-1}[X] \times \mathbf{A}_{p-1}[X]$ tel que

$$\mathrm{Res}(P, Q) \quad = \quad UP + VQ \quad = \quad (U\overline{P} + V\overline{Q})\Delta$$

Or (voir remarque 2.3), $\deg \mathrm{Res}(P, Q) \leq 1$, donc

$$U\overline{P} + V\overline{Q} = 0$$

On en déduit donc $\mathrm{Res}(P, Q) = 0$. □

Lemme 2.8. *Soit $f \in \mathbb{Z}[X]$. On a*

$$\mathrm{Res}(f, f') = 0 \iff \mathrm{Res}(\hat{f}, \hat{f}') = 0$$

où $\hat{f}$ est le réduit de f, défini au lemme 2.4.

Démonstration. L'anneau $\mathbb{Z}$ étant factoriel, on peut utiliser le lemme 2.7. Dès lors, le discriminant de f est nul si et seulement si f admet un facteur carré. Autrement dit, le discriminant de f est nul si et seulement s'il existe $I \in \mathbb{Z}[X]$ irréductible tel que $f = I^2 g$, pour un certain $g \in \mathbb{Z}[X]$. Par l'identité (2) de la démonstration du lemme 2.5, on a que $\hat{f}$ admet un facteur carré, et donc $\mathrm{Res}(\hat{f}, \hat{f}')$ est nul. La réciproque découle de façon analogue de l'identité (1) de la même démonstration. □

Théorème 2.2 (Calcul du résultant par l'algorithme d'Euclide)**.** *Soit $\mathbf{A}$ un anneau factoriel. Soient $P, Q \in \mathbf{A}[X]$. On suppose que le coefficient dominant b_m de Q est inversible dans $\mathbf{A}$. On suppose de plus $n = \deg P \geq \deg Q = m$ On note R le reste de la division euclidienne de P par Q dans $\mathbf{A}$. On note de plus $r = \deg R$.*

1. *Si $R = 0$, alors* $\mathrm{Res}(P, Q) = 0$
2. *Si $R \neq 0$, alors* $\mathrm{Res}(P, Q) = b_m^{n-r}(-1)^{nm}\mathrm{Res}(Q, R)$

Démonstration. Le premier point est immédiat par le lemme 2.7. On suppose dorénavant $R \neq 0$. Sans perdre de généralité, on a supposé $n \geq m$. Le cas contraire implique $R = P$ et on conclut par les propriétés du résultant (lemme 2.6), sans le facteur b_m. Sous ces hypothèses, $P = TQ + R$ pour un certain polynôme non nul $T \in \mathbf{A}[X]$. On note $Q = \sum_{k=0}^{m} b_k X^k$, $T = \sum_{k=0}^{s} t_k X^k$, $R = \sum_{k=0}^{m-1} r_k X^k$, avec $r_j = 0$ pour tout $j > r$, et $s = n - m$. Alors i-ième

colonne de la matrice de Sylvester associée à P, Q, pour $1 \leq i \leq m$ s'écrit

$$S_i = \begin{pmatrix} 0 \\ | \\ 0 \\ t_s b_m \\ t_s b_{m-1} + t_{s-1} b_m + r_{m-1} \\ t_s b_{m-2} + t_{s-1} b_{m-1} + t_{s-2} b_m + r_{m-2} \\ | \\ t_0 b_0 + r_0 \\ 0 \\ | \\ 0 \end{pmatrix}$$

Cette colonne s'écrit alors

$$S_i = t_s \times S_{m+i} + t_{s-1} \times S_{m+i+1} + ... + t_0 \times S_{n+i} + R_i$$

où R_i est une colonne ne dépendant que des coefficients de R. Dès lors, le résultant s'écrit :

$$\text{Res}(P, Q) = \det(R_1 | R_2 | ... | R_m | S_{m+1} | ... | S_{m+n})$$

puisque les colonnes sont liées en présence d'une colonne S_i, $1 \leq i \leq m$.

On développe ensuite par rapport à le première ligne : il ne reste plus que b_m à la $(m+1)$-ième ligne :

$$\text{Res}(P, Q) = b_m (-1)^m \times \det\left(R'_1 | ... | R'_m | S'_m | ... | S'_{m+n}\right)$$

avec des notations implicites. Si $r_{m-1} = 0$, on développe encore. On continue à développer tant que $r_j = 0$, jusque arriver à $r_r \neq 0$ après $n - r$ développements. On obtient alors :

$$\text{Res}(P, Q) = b_m^{n-r} (-1)^{m(n-r)} \text{Res}(R, Q) = b_m^{n-r} (-1)^{nm} \text{Res}(Q, R)$$

□

Remarque 2.4. Mis à part le coefficient $b_m^{n-r}(-1)^{nm}$, cette expression du résultant est analogue à celle du pgcd de deux polynômes lors du calcul par l'algorithme d'Euclide. C'est à ce titre que nous dirons que nous calculons le résultant par l'algorithme d'Euclide.

L'hypothèse sur le coefficient dominant de Q permet la division euclidienne dans $\mathbf{A}$, puisqu'on ne suppose pas que $\mathbf{A}$ est euclidien. D'un point de vue algorithmique, ceci n'est pas garanti lors de la procédure. Il y a deux manières de contourner ce problème lorsque l'on travaille dans un anneau euclidien : on peut effectuer les calculs dans le corps des fractions $Frac(\mathbf{A})$, ou on peut effectuer des **pseudo-divisions** (voir la source [4] pour cette deuxième possibilité).

Le calcul du résultant prouvera important dans les prochaines sections. L'utilisation du pivot de Gauss provoquera un calcul ayant une complexité en temps de l'ordre $O((n+m)^3)$, tandis que l'algorithme d'Euclide précédent a une complexité quadratique.

Théorème 2.3 (Expression du résultant par les racines)**.** *Soit* $\mathbf{A}$ *un anneau euclidien. Soit* $\mathbf{K}$ *un sur-corps de* $\mathbf{A}$ *algébriquement clos. Soient* $P = a_n \prod_{i=1}^{n}(X - \alpha_i), Q = b_m \prod_{j=1}^{m}(X - \beta_j) \in \mathbf{A}[X]$*, où les* α_i, β_j *sont les racines dans* $\mathbf{K}$*. On a l'expression suivante du résultant :*

$$\mathrm{Res}(P,Q) = a_n^m b_m^n \prod_{1\le i\le n, 1\le j\le m} (\alpha_i - \beta_j)$$

Démonstration. Définissons l'application

$$\begin{aligned} \Phi : \quad & \mathbf{A}[X] \times \mathbf{A}[X] \to \mathbf{K} \\ & (P,Q) \mapsto a_n^m \prod_{i=1}^{n} Q(\alpha_i) \end{aligned}$$

Nous allons montrer que le calcul de $\Phi(P,Q)$ se fait exactement de la même manière que le calcul de $\mathrm{Res}(P,Q)$. Commençons par démontrer quelques propriétés de Φ :

1. $\Phi(\alpha, Q) = \alpha^m$ pour tout $\alpha \in \mathbf{A}$.
   En effet, le produit (vide) vaut $1_{\mathbf{A}}$, et le coefficient dominant de P est α.
2. $\Phi(P,Q) = (-1)^{nm}\Phi(Q,P)$.
   On a :

$$\begin{aligned} \Phi(P,Q) &= a_n^m \prod_{i=1}^{n} Q(\alpha_i) \\ &= a_n^m \prod_{i=1}^{n} b_m \prod_{j=1}^{m} (\alpha_i - \beta_j) \\ &= b_m^n (-1)^{nm} \prod_{j=1}^{m} P(\beta_j) \quad = \quad (-1)^{nm}\Phi(Q,P) \end{aligned}$$

On remarque déjà des propriétés analogues à celles du résultant. Montrons alors la relation du théorème précédent, mais pour Φ au lieu de Res. Notons R le reste de la division euclidienne de P par Q dans $\mathbf{A}[X]$, et T le quotient. Si $R = 0$, alors $\Phi(P,Q) = 0$, car P et Q admettent un facteur commun non trivial dans $\mathbf{A}[X]$ (lemme 2.7), et donc une racine dans $\mathbf{K}$. Si $R \neq 0$, montrons l'identité :

$$\Phi(P,Q) = b_m^{n - \deg R} (-1)^{nm} \Phi(Q,R) \tag{3}$$

On a, en notant $r = \deg R$:

$$\begin{aligned} \Phi(P,Q) &= (-1)^{nm}\Phi(Q, TQ + R) \\ &= (-1)^{nm} b_m^n \prod_{j=1}^{m} (TQ + R)(\beta_j) \\ &= (-1)^{nm} b_m^n \prod_{j=1}^{m} R(\beta_j) \\ &= (-1)^{nm} b_m^{n-r} \Phi(Q,R) \end{aligned}$$

Ainsi, le même algorithme calcule $\mathrm{Res}(P,Q)$ et $\Phi(P,Q)$: ces deux valeurs sont donc égales, d'où :

$$\mathrm{Res}(P,Q) = a_n^m \prod_{i=1}^{n} Q(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} P(\beta_j) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

□

Exemple. Prenons les polynômes

$$P = \frac{X^p - 1}{X - 1}, \quad Q = \frac{X^q - 1}{X - 1}$$

pour p, q deux nombres premiers distincts. Alors :

$$\mathrm{Res}(P,Q) = \prod_{k=1}^{p-1} \left(\frac{\exp\left[\frac{2i\pi}{p} qk\right] - 1}{\exp\left[\frac{2i\pi}{p} k\right] - 1} \right) \in \mathbb{Z}$$

ce qui est bien un entier relatif car ces deux polynômes sont des éléments de $\mathbb{Z}[X]$.

Exemple. Le résultant permet de démontrer plusieurs résultats sur $\overline{\mathbb{Q}}$, l'ensemble des entiers algébriques. Cet ensemble est défini comme le sous-ensemble de $\mathbb{C}$ constitué de racines de polynômes de $\mathbb{Q}[X]$.

Si $x \in \overline{\mathbb{Q}}$, on pose :

$$I_x = \{P \in \mathbb{Q}[X] : P(x) = 0\}$$

et on vérifie qu'il s'agit d'un idéal non nul de $\mathbb{Q}[X]$. Il est donc engendré par un unique polynôme unitaire Π_x, que l'on appelle polynôme minimal de x.

Soient $x, y \in \overline{\mathbb{Q}}$. Montrons que $x + y \in \overline{\mathbb{Q}}$. On note P, Q les polynômes minimaux respectifs de x, y. On note $z = x + y$, et on pose $R = Q(z - X)$. Alors

$$\mathrm{Res}(P,R) = a_n^m \prod_{i=1}^{n} Q(z - \alpha_i) = a_n^m Q(x + y - x) \prod_{i=1}^{n} Q(z - \alpha_i) = 0$$

Or $Y \mapsto \mathrm{Res}(P, Q(Y - X))$ est un polynôme en Y à coefficients dans $\mathbb{Q}$, et qui s'annule en z, donc $z \in \overline{\mathbb{Q}}$.

De plus, on note $t = xy$, et on a

$$\mathrm{Res}\left(P, X^p Q\left(\frac{t}{X}\right)\right) = 0$$

puisque les deux s'annulent en x. Or il s'agit d'un polynôme à coefficients rationnels en t, ce qui implique $t \in \overline{\mathbb{Q}}$.

Le résultant permet ainsi de montrer que $\overline{\mathbb{Q}}$ est un corps.

2.3 Majoration des coefficients d'un facteur

Dans toute la suite, $||f||$ désigne la norme 2 du polynôme $f = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, définie par :

$$||f|| \quad = \quad \sqrt{|a_1|^2 + |a_2|^2 + ... + |a_n|^2}$$

Définition 2.6 (Mesure)**.** *Soit $f = \sum_{k=0}^{n} \in \mathbb{C}[X]$. On note $z_1, ..., z_n$ les racines complexes non nécessairement distinctes de f. On appelle* ***mesure*** *de f le réel :*

$$M(f) \quad := \quad |a_n| \prod_{i=1}^{n} \max(1, |z_i|)$$

Lemme 2.9 (Premières propriétés)**.** *Soient $f, g \in \mathbb{C}[X]$. La mesure de vérifie :*

1. $M(fg) = M(f)M(g)$
2. $\max |a_j| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} M(f)$

où $\lfloor x \rfloor$ désigne la partie entière de $x \in \mathbb{R}$, et a_j est le j-ième coefficient de f.

Démonstration. Le premier résultat est immédiat. Quant au deuxième, on utilise les formules de Viète liant coefficients et racines :

$$a_j \quad = \quad (-1)^{n-j} a_n \times \sum_{1 \leq k_1 < ... < k_j \leq n} z_{k_1} ... z_{k_j}$$

et on en déduit alors :

$$|a_j| \quad \leq \quad \binom{n}{j} M(f) \quad \leq \quad \binom{n}{\lfloor \frac{n}{2} \rfloor} M(f)$$

□

Lemme 2.10. *Soit $f \in \mathbb{C}[X]$. Pour tout nombre complexe z, on a :*

$$||(X - z)f|| = ||(\overline{z}X - 1)f||$$

Démonstration. On a l'égalité

$$||Q||^2 \quad = \quad \frac{1}{2\pi} \int_0^{2\pi} |Q(e^{it})|^2 dt$$

pour tout $Q \in \mathbb{C}[X]$. En effet,

$$\int_0^{2\pi} e^{ikt} dt \quad = \quad \begin{cases} 0 & \text{si } k \neq 0 \\ 2\pi & \text{sinon} \end{cases}$$

puis :

$$\begin{aligned}\frac{1}{2\pi}\int_0^{2\pi}|Q(e^{it})|^2dt &= \frac{1}{2\pi}\int_0^{2\pi}|a_ne^{int}+...+a_0|^2dt\\ &= \frac{1}{2\pi}\int_0^{2\pi}(a_ne^{int}+...+a_0)\overline{(a_ne^{int}+...+a_0)}dt\\ &= \frac{1}{2\pi}\sum_{j=0}^{n}\sum_{k=0}^{n}\int_0^{2\pi}a_j\overline{a_k}e^{it(j-k)}dt\\ &= \frac{1}{2\pi}\sum_{k=0}^{n}\int_0^{2\pi}|a_k|^2dt \quad = \quad ||Q||^2\end{aligned}$$

Dès lors, pour $Q := (X-z)f$, on a :

$$\begin{aligned}||(X-z)f||^2 &= \frac{1}{2\pi}\int_0^{2\pi}|e^{it}-z|^2\times|f(e^{it})|^2dt\\ &= \frac{1}{2\pi}\int_0^{2\pi}|1-\overline{z}e^{it}|\times|f(e^{it})|^2dt\\ &= ||(\overline{z}X-1)f||^2\end{aligned}$$

□

Théorème 2.4 (Inégalité de Mignotte-Landau)**.** *On a l'inégalité :*

$$M(f) \quad \leq \quad ||f||$$

Démonstration. Notons $I := \{1 \leq i \leq n \ : \ 1 < |z_i|\}$. Alors :

$$M(f) \quad = \quad |a_n|\prod_{i\in I}|z_i|$$

On pose :

$$Q \quad := \quad \prod_{i\in I}(\overline{z_i}X-1)\times\prod_{i\notin I}(X-z_i)$$

Par une itération du lemme précédent, on a que $||Q|| = ||f||$. Par construction, on a de plus que $M(Q)$ est égal au module du coefficient dominant de Q, i.e :

$$M(Q) \quad = \quad \prod_{i\in I}|z_i| \quad = \quad M(f)$$

On conclut alors en majorant le module du coefficient dominant de Q par $||Q||$.
□

Corollaire 2.4.1 (Majoration des coefficients d'un facteur de f)**.** *Si g est un facteur de de f, et de coefficient dominant b_k, alors :*

$$||g|| \quad \leq \quad \sqrt{k+1}\binom{k}{\lfloor\frac{k}{2}\rfloor}\times\frac{|b_k|}{|a_n|}\times||f||$$

Démonstration. Par le lemme 2.9, on a :

$$||g|| \quad \leq \quad \sqrt{k+1}\binom{k}{\lfloor \frac{k}{2} \rfloor} M(g)$$

En notant $f = gh$, on a $M(f) = M(g)M(h)$, et $M(h) \geq |\mathrm{cd}(h)|$, coefficient dominant de h. Or $a_n = b_k \times \mathrm{cd}(h)$, donc :

$$M(f) \quad \geq \quad \frac{|a_n|}{|b_k|} M(g)$$

On en déduit donc

$$||g|| \quad \leq \quad \sqrt{k+1}\binom{k}{\lfloor \frac{k}{2} \rfloor} \times \frac{|b_k|}{|a_n|} \times ||f||$$

par le lemme 2.4. □

Corollaire 2.4.2 (Majoration des coefficients d'un facteur de f dans $\mathbb{Z}[X]$)**.** *Si f, g sont à coefficients entiers, alors avec les mêmes notations :*

$$||g|| \quad \leq \quad \sqrt{k+1}\binom{k}{\lfloor \frac{k}{2} \rfloor} ||f||$$

Démonstration. Il suffit de remarquer que b_k divise a_n : comme il s'agit d'entiers relatifs non nuls, on en déduit que $|b_k| \leq |a_n|$. □

3 Lemme de Berlekamp

Dans cette partie, p désigne un nombre premier.

3.1 Étude de l'algèbre de Berlekamp

Définition 3.1 (Algèbre de Berlekamp)**.** *Soit $f \in \mathbb{F}_p[X]$. On note*

$$\begin{aligned} S :\ & \mathbb{F}_p[X]/(f) \to \mathbb{F}_p[X]/(f) \\ & a \mapsto a^p - a \end{aligned}$$

On appelle ***algèbre de Berlekamp*** *le noyau de cet endomorphisme de $\mathbb{F}_p$-espace vectoriel.*

Démonstration. Montrons que S est bien un endomorphisme, et que $\ker S$ est une sous-$\mathbb{F}_p$-algèbre de $\mathbb{F}_p[X]/(f)$. Soient $a, b \in \mathbb{F}_p[X]/(f)$, $\alpha, \beta \in \mathbb{F}_p$. On a, dans $\mathbb{F}_p$

$$\begin{aligned} S(\alpha a + \beta b) &= (\alpha a + \beta b)^p - \alpha a - \beta b \\ &= \sum_{k=0}^{p} \binom{p}{k} \alpha^k a^k \beta^{p-k} b^{p-k} - \alpha a - \beta b \\ &= (\alpha^0 a^0 \beta^p b^p + \alpha^p a^p \beta^0 b^0) - \alpha a - \beta b \\ &= \alpha S(a) + \beta S(b) \end{aligned}$$

Donc S est bien linéaire. De plus, si $a, b \in \ker S$, alors

$$(ab)^p - (ab) = a^p b^p - ab = ab - ab = 0$$

donc $ab \in \ker S$. Enfin, $1 \in \ker S$. □

Théorème 3.1 (Lemme de Berlekamp)**.** *Soit $f \in \mathbb{F}_p[X]$ sans facteurs carrés. Pour tout g dans l'algèbre de Berlekamp $\ker S$, on a l'égalité dans $\mathbb{F}_p[X]$:*

$$f = \prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(g - \alpha, f)$$

Démonstration. Les $g - \alpha$ sont deux à deux premiers entre eux dans $\mathbb{F}_p[X]$ (par exemple, en écrivant une relation de Bézout). Dès lors, on a :

$$\prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(g - \alpha, f) = \operatorname{pgcd}(\prod_{\alpha \in \mathbb{F}_p} (g - \alpha), f)$$

Posons $M := \prod_{\alpha \in \mathbb{F}_p} (X - \alpha) \in \mathbb{F}_p[X]$. Alors M est de degré p, unitaire, et nul sur $\mathbb{F}_p[X]$. On en déduit l'égalité dans $\mathbb{F}_p[X]$:

$$M = X^p - X$$

d'où

$$\prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(g - \alpha, f) = \operatorname{pgcd}(M \circ g, f) = \operatorname{pgcd}(0, f) = f$$

car $g \in \ker S$. □

Si $g \in \ker S$ est non trivial, alors on a $1 \leq \deg g < \deg f$, ce qui implique qu'au moins un des $\text{pgcd}(g - \alpha, f)$ est non trivial par le lemme de Berlekamp. Par conséquent, le lemme de Berlekamp permet bien de factoriser un polynôme de $\mathbb{F}_p[X]$.

Lemme 3.1. *Soit f sans facteurs carrés. Si $f = f_1 f_2 ... f_r$ est la décomposition sans facteurs carrés de f dans $\mathbb{F}_p[X]$, alors l'algèbre de Berlekamp $\ker S$ est de dimension r.*

Démonstration. Par le théorème de l'isomorphisme chinois, que l'on peut appliquer puisque l'on suppose f sans facteurs carrés, on dispose de

$$\phi : \mathbb{F}_p[X]/(f) \to \prod_{i=1}^{r} \mathbb{F}_p[X]/(f_i)$$

un isomorphisme de $\mathbb{F}_p$-algèbres. Si $g = (g_i)_{1 \leq i \leq r} \in \mathbb{F}_p[X]/(f)$ a toutes ses composantes constantes, alors $g \in \ker S$ de façon immédiate. Réciproquement, si g est dans l'algèbre de Berlekamp, alors

$$\forall i \in \{1, ..., r\}, \quad g_i^p - g_i = 0$$

ce qui implique, par l'identité :

$$X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha)$$

que

$$\forall i \in \{1, ..., r\}, \quad \prod_{\alpha \in \mathbb{F}_p} (X - \alpha) \equiv 0 \mod f_i$$

Dès lors, chaque f_i divise au moins un des $g_i - \alpha$, et $g_i \in \mathbb{F}_p[X]/(f_i)$, donc

$$\forall i \in \{1, ..., r\}, \quad g_i \text{ est constant}$$

On aurait aussi pu utiliser le lemme de rupture : sachant que $\mathbb{F}_p[X]/(f_i)$ est un sur-corps de $\mathbb{F}_p$, les seuls éléments x de $\mathbb{F}_p[X]/(f_i)$ vérifiant $x^p = x$ sont dans $\mathbb{F}_p$ (car $X^p - X$ admet au plus p racines dans ce corps, et est nul sur les p éléments de $\mathbb{F}_p$). On retrouve que g_i est constant. Dès lors,

$$\text{Card } \ker S \quad = \quad \text{Card } \mathbb{F}_p^r \quad = \quad p^r$$

Donc $\ker S$ est bien de dimension r. □

L'hypothèse « sans facteurs carrés » sert notamment à assurer la correction de l'algorithme : grâce à cette hypothèse, on dispose du lemme précédent, et celui-ci assure que l'algorithme renvoie la factorisation triviale si et seulement si f est irréductible dans $\mathbb{F}_p[X]$.

3.2 Algorithme

Implémentation algorithmique 1 (Berlekamp)**.** *Soit* $f \in \mathbb{F}_p[X]$*. Pour* $i \in \{0, ..., \deg f - 1\}$*, on détermine les coefficients* $s_{i,1}, ..., s_{i,\deg f-1} \in \mathbb{F}_p[X]$ *tels que*

$$x^{ip} - x^i \quad \equiv \quad \sum_{j=0}^{\deg f - 1} s_{i,j} x^j \mod f$$

Il s'agit d'effectuer $\deg f - 1$ *divisions euclidiennes de polynômes de degré au plus* $(\deg f - 1)p$ *par un polynôme de degré* $\deg f$*. On définit ainsi la matrice* $(s_{i,j})$ *de* S *dans la base* $(1, x, ..., x^{\deg f - 1})$*. On recherche ensuite, par le pivot de Gauss, un élément du noyau de* S*. Concrètement, on décompose la factorisation dans* $\mathbb{F}_p[X]$ *en :*

1. *Construction de la matrice* S *par des divisions euclidiennes dans* $\mathbb{F}_p[X]$*.*
2. *Calcul du noyau de* S *par la méthode du pivot de Gauss.*
3. *Si le noyau est de cardinal* p*, on renvoie la factorisation triviale.*
4. *Sinon, on renvoie un* $\text{pgcd}(g - \alpha, f)$ *non trivial.*

Entrées : $f \in \mathbb{Z}[X]$ unitaire, p premier
Sorties : $G, H \in \mathbb{Z}[X]$ unitaires et premiers entre eux tels que $f = GH \mod p$

Faire
  $n \leftarrow \deg f$
  for $i = 0$ *to* $n - 1$ **do**
    $(s_{i,0}, ..., s_{i,n-1}) \leftarrow \text{coefs}(Reste\_Div\_Euclide(x^{ip} - x^i, f))$
  $S \leftarrow (s_{i-1,j-1})_{1 \leq i,j \leq n}$
  $v \leftarrow$ vecteur de ker S
  si $\deg v \geq 1$ **alors**
    $g \leftarrow \text{pgcd}(f, v - \alpha)$ où $\text{pgcd}(f, v - \alpha)$ est non trivial
    Rendre g, $Quotient\_Div\_Euclide(f, g)$
  sinon
    f est irréductible
    Rendre $f, 1$

Pseudo-code 3.1 (Procédure BERLEKAMP)**.**

Nous chercherons, lors de l'implémentation en OCaml, à faire en sorte que le vecteur prit dans $\ker S$ est constant si et seulement si f est irréductible sur $\mathbb{F}_p[X]$.

4 Lemme de Hensel

4.1 Énoncé et preuve

Lemme 4.1 (Lemme de Hensel)**.** *Soit $f \in \mathbb{Z}[X]$ unitaire. Soient $G, H \in \mathbb{Z}[X]$ unitaires et premiers entre eux. Soit p premier. On suppose que*

$$f = GH \mod p$$

Alors, pour tout $k \in \mathbb{N}$, il existe $G_k, H_k \in \mathbb{Z}[X]$ unitaires et premiers entre eux tels que $\deg f = \deg H_k + \deg G_k$ *et :*

$$\begin{aligned} G_k &\equiv G \mod p^{2^k} \\ H_k &\equiv H \mod p^{2^k} \\ f &\equiv G_k H_k \mod p^{2^k} \end{aligned}$$

Démonstration du lemme de Hensel. On raisonne par récurrence sur $k \in \mathbb{N}$. L'initialisation est assurée par les hypothèses du lemme. Soit $k \in \mathbb{N}$. On suppose disposer de $G_k, H_k, U_k, V_k \in \mathbb{Z}[X]$ unitaires tels que

$$\begin{aligned} f &= G_k H_k \mod p^{2^k} \\ U_k G_k + V_k H_k &= 1 \mod p^{2^k} \\ \deg U_k &< \deg G_k \\ \deg V_k &< \deg H_k \end{aligned}$$

La deuxième équation revient à l'hypothèse « G_k, H_k sont premiers entre eux ». Pour alléger les notations, on note $K := 2^k$. On définit $R_k \in \mathbb{Z}[X]$ comme unitaire et vérifiant :

$$f = G_k H_k + p^K R_k \mod p^{2K}$$

On cherche à résoudre le système d'inconnue $(g_k, h_k) \in \mathbb{Z}[X]^2$:

$$\begin{cases} G_{k+1} = G_k + p^K g_k \\ H_{k+1} = H_k + p^K h_k \end{cases} \tag{4}$$

Des solutions de (4) vérifient alors :

$$\begin{aligned} f &= G_{k+1} H_{k+1} && \mod p^{2K} \\ &= (G_k + p^K g_k)(H_k + p^K h_k) && \mod p^{2K} \\ &= G_k H_k + p^K (H_k g_k + G_k h_k) && \mod p^{2K} \\ &= G_k H_k + p^K R_k && \mod p^{2K} \end{aligned}$$

Il suffit donc de prendre

$$\begin{aligned} H_k g_k + G_k h_k &= R_k \\ H_k g_k &= R_k \quad \mod G_k \\ V_k H_k g_k &= V_k R_k \quad \mod G_k \\ (1 - U_k G_k) g_k &= V_k R_k \quad \mod G_k \\ g_k &= V_k R_k \quad \mod G_k \end{aligned}$$

et de même pour h_k. On pose donc :

$$\begin{aligned} G_{k+1} &:= G_k + p^K (V_k R_k \mod G_k) \\ H_{k+1} &:= H_k + p^K (U_k R_k \mod H_k) \end{aligned} \tag{5}$$

On a notamment la conservation du On obtient des formules similaires pour U_{k+1}, V_{k+1} (non démontrées ici). Le principe est de passer de l'inverse de G_k modulo H_k à l'inverse de G_{k+1}. □

Ayant supposé G, H unitaires, la division euclidienne se fait aisément dans $\mathbb{Z}[X]$ et ne posera pas de soucis lors de l'algorithme.

4.2 Algorithme HENSEL

Entrées : $f, g_k, h_k, u_k, v_k \in \mathbb{Z}[X]$
Sorties : $g_{2k}, h_{2k}, u_{2k}, v_{2k} \in \mathbb{Z}[X]$

Faire
- $r \leftarrow \frac{1}{p^k}(f - g_k h_k)$
- $h_{2k} \leftarrow h_k + p^k \times Reste\_Div\_Euclide(u_k r, h_k)$
- $g_{2k} \leftarrow g_k + p^k \times Reste\_Div\_Euclide(v_k r, g_k)$
- $u_{2k} \leftarrow Reste\_Div\_Euclide(2u_k - u_k^2 g_{2k}, h_{2k})$
- $v_{2k} \leftarrow Reste\_Div\_Euclide(2v_k - v_k^2 h_{2k}, g_{2k})$

Rendre $g_{2k}, h_{2k}, u_{2k}, v_{2k}$

Pseudo-code 4.1 (HENSEL)**.**

4.3 Un invariant

Lemme 4.2. *La fonction HENSEL ci-dessus admet la propriété suivante :*

$$(g_{2k}, h_{2k}) = (f, 1) \text{ si et seulement si } (g_k, h_k) = (f, 1)$$

Démonstration. Commençons par le sens indirect. Supposons $(g_k, h_k) = (f, 1)$. On rappelle que les polynômes sont dans $\mathbb{Z}[X]$: On a alors $r = 0$. Dès lors, par le pseudo-code précédent, $h_{2k} = h_k = 1$, et $g_{2k} = g_k = f$.

Réciproquement, on suppose que $(g_k, h_k) \neq (f, 1)$. Alors on a deux cas :

1er cas : $r = 0$
Dans ce cas, par application de l'algorithme, $(h_{2k}, g_{2k}) = (h_k, g_k) \neq (f, 1)$.

2e cas : $r \neq 0$
Dans ce cas, dire que $h_{2k} = 1$ signifierait

$$h_k = 1 - p^k \times Reste\_Div\_Euclide(u_k r, h_k)$$

À cause des inégalités sur les degrés, on aurait alors ou bien $\deg h_k < \deg h_k$, ou bien $h_k = 0$. Les deux cas sont absurdes (sauf si f est nul, mais il est supposé unitaire), donc $h_{2k} \neq 1$, et on conclut.

On a donc bien l'équivalence. □

5 Factorisation dans $\mathbb{Z}[X]$

Dans toute la suite, on fixe un polynôme $f = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Quitte à passer à son réduit $\hat{f}$, défini au lemme 2.4, on suppose f unitaire. On suppose de plus f sans facteurs carrés dans $\mathbb{Z}[X]$: sinon, il suffirait de prendre $\text{pgcd}(f, f')$ qui serait non trivial.

5.1 Choix de p

On cherche en premier lieu à appliquer le lemme de Berlekamp. Pour ce faire, il faut choisir un nombre premier convenable. L'hypothèse principale demande à ce que f soit sans facteurs carrés. Nous disposons de la caractérisation par le lemme 2.7, que l'on applique à

$$\overline{f} \quad := \quad \sum_{k=0}^{n} \overline{a_k} X^k \in \mathbb{F}_p[X]$$

où les $\overline{a_k}$ sont les classes respectives des a_k dans $\mathbb{F}_p$. Alors $\overline{f}$ est sans facteurs carrés dans $\mathbb{F}_p[X]$ si et seulement si

$$\overline{\text{Res}(f, f')} = \text{Res}(\overline{f}, \overline{f'}) = 0 \quad (\text{dans } \mathbb{F}_p)$$

Il s'agit donc de choisir un nombre premier ne divisant pas l'entier $\text{Res}(f, f')$. On cherche à majorer la valeur d'un tel p.

Lemme 5.1 (Inégalité d'Hadamard)**.** *Soit M une matrice carrée réelle. On note $X_1, ..., X_n$ ses colonnes, et $||X||_2 := \sqrt{|x_1|^2 + ... + |x_n|^2}$ lorsque $x_1, ..., x_n$ sont les coordonnées de X. Alors :*

$$|\det M| \leq ||X_1||_2 ... ||X_n||_2$$

Démonstration. Si $(X_1, ..., X_n)$ est liée, alors le déterminant est nul et l'inégalité est vérifiée. On suppose dorénavant que cette famille est libre. Il s'agit alors

d'une base de $\mathbb{R}^n$. Par le procédé d'orthonormalisation de Gram-Schmidt, on peut construire une base orthonormale $(E_1, ..., E_n)$ telle que

$$\forall i \in \{1, ..., n\}, \quad vect(X_1, ..., X_p) = vect(E_1, ..., E_n)$$

Alors la matrice de passage P de $(E_1, ..., E_n)$ à $(X_1, ..., X_n)$ est triangulaire supérieure, et ses coefficients diagonaux sont les $\langle X_i, E_i \rangle$. M est la matrice de passage de la base canonique dans la base $(X_1, ..., X_n)$, donc en notant E la matrice $(E_1|...|E_n)$, on a :

$$M = EP$$

Dès lors,

$$|\det M| = |\det P| = |\langle X_1, E_1 \rangle|...|\langle X_n, E_n \rangle|$$

et on conclut par application de l'inégalité de Cauchy-Schwarz. □

Lemme 5.2 (Majoration du résultant)**.** *Si $P, Q \in \mathbb{Z}[X]$, alors :*

$$\mathrm{Res}(P, Q) \leq ||P||_2^m \times ||Q||_2^n \leq (\sqrt{n}||P||_\infty)^m \times (\sqrt{m}||Q||_\infty)^n$$

où $||P||_\infty$ désigne la norme infinie.

Démonstration. La première inégalité découle de l'inégalité d'Hadamard. La deuxième est une majoration des coefficients sous la racine carrée de la norme deux par la norme infinie. □

Il reste cependant à discuter du nombre de facteurs premiers distincts qui peuvent diviser le résultant. À ce titre, on va utiliser le théorème des nombres premiers :

Théorème 5.1 (Théorème des nombres premiers)**.**

$$\sum_{p \leq m} \ln p \sim m$$

où la somme porte sur l'ensemble des nombre premiers inférieurs ou égaux à $m \in \mathbb{N}$.

Démonstration. Admise. □

On a donc

$$\prod_{p \leq m} p \geq e^{\frac{m}{2}}$$

pour m suffisamment grand.

Lemme 5.3. $\mathrm{Res}(f, f')$ *ne peut pas admettre plus de $\pi(4n \ln n + 4n \ln ||f||_\infty)$ facteurs premiers distincts, où $\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x.*

Démonstration. Appliquons le lemme 5.2 à f et à f'. On a :

$$\mathrm{Res}(f, f') \leq (\sqrt{n}||f||_\infty)^{n-1}(n\sqrt{n}||f||_\infty)^n$$

On en déduit donc

$$\mathrm{Res}(f, f') \leq n^{2n}||f||_\infty^{2n}$$

Dès lors, pour tout m tel que $e^{\frac{m}{2}} \geq \mathrm{Res}(f, f')$, on a

$$\prod_{p \leq m} p \geq \mathrm{Res}(f, f')$$

Ainsi, il suffit de prendre $m \geq 4n \ln n + 4n \ln ||f||_\infty$, ce qui démontre le résultat. □

On admet de plus l'équivalent

$$\pi(x) \sim \frac{x}{\ln x}$$

Pour des paramètres n et $||f||_\infty$ suffisamment grands, on a donc

$$\pi(4n \ln n + 4n \ln ||f||_\infty) \leq 8 \frac{n \ln n + n \ln ||f||_\infty}{\ln(4n \ln n + 4n \ln ||f||_\infty)}$$

Lemme 5.4. *On note $\theta(f)$ nombre maximal de facteurs premiers distincts de* $\mathrm{Res}(f, f')$. *On a l'ordre de grandeur :*

$$\theta(f) = O\left(\frac{n}{\ln n} \frac{\ln ||f||_\infty}{\ln \ln ||f||_\infty + \ln \ln n}\right) = O\left(\frac{n}{\ln n} \ln ||f||_\infty\right)$$

en assimilant $\ln \ln ||f||_\infty$ *et* $\ln \ln n$ *à des constantes.*

Démonstration. Découle immédiatement des commentaires précédents. □

On procède alors à une recherche de nombre premiers ne divisant pas $\mathrm{Res}(f, f')$. On cherche à calculer les premiers nombre premiers jusqu'à en obtenir un ne divisant pas $\mathrm{Res}(f, f')$. En vertu de l'ordre de grandeur précédent, il suffira de calculer les

$$N(f) := 8 \left\lceil \frac{n}{\ln n} \ln ||f||_\infty \right\rceil + 1$$

premiers nombre premiers. Il y aura parmi eux au moins un nombre premier ne divisant pas $\mathrm{Res}(f, f')$. En moyenne, il y aura bien moins de calculs à faire, puisqu'il sera (à priori) très rare de tomber sur un polynôme dont le résultant $\mathrm{Res}(f, f')$ n'admette pas de facteurs carrés.

Nous discuterons plus longuement de la complexité lors de l'implémentation en OCaml.

Dans la suite, la fonction qui renvoie un nombre premier ne divisant le résultant sera notée Non_Div_Prime.

5.2 Arrêt de la remontée par HENSEL

Selon le corollaire 2.4.2, on peut arrêter la remontée de Hensel dès que p^K dépasse une certaine valeur. Autrement dit, si $k := \deg g$ pour g facteur de f modulo p^{2^r}, alors on peut arrêter la remontée dès que :

$$2^r \quad \geq \quad \left\lceil \frac{1}{2}\log_p(k+1) + \log_p \binom{k}{\lfloor \frac{k}{2} \rfloor} + \log_p ||f|| \right\rceil$$

Ceci constitue une condition d'arrêt de la remontée. Notamment, la remontée a lieu au plus r fois, avec :

$$r \quad := \quad \left\lceil \log_2 \frac{1}{2}\log_p(k+1) + \log_p \binom{k}{\lfloor \frac{k}{2} \rfloor} + \log_p ||f|| \right\rceil$$

Lemme 5.5. *On note $K = 2^r$. Prenons $g, h \in \mathbb{Z}[X]$ tels que $f = gh \mod p^K$. On prend les coefficients de g, h dans $]-p^K/2\ ;\ p^K/2[$. Alors, nous disposons de l'alternative suivante :*

1. *ou bien* $\text{pgcd}(f,g)$ *ou* $\text{pgcd}(f,h)$ *est non trivial.*
2. *ou bien* $\{g,h\} = \{f,1\}$.

Ce lemme montre qu'il est bien suffisant d'arrêter la remontée de Hensel à partir du rang K.

Démonstration. Supposons que $\{g,h\} \neq \{f,1\}$. Soit P un facteur irréductible de f. On note $f = PQ$, et $k = \deg P \leq n = \deg f$. Alors selon les hypothèses :

$$PQ = gh \mod p^K$$

On décompose g, h en produit d'irréductibles de $\mathbb{Z}[X]$: $g = G_1...G_s$, $h = H_1...H_t$. Dès lors :

$$PQ = G_1...G_sH_1...H_t \mod p^K$$

Nous avons cependant que (voir la section 2.3) :

$$||P||_\infty \quad \leq \quad \sqrt{n+1}\binom{n}{\lfloor n/2 \rfloor}||f||_2 \quad < \quad \frac{p^K}{2}$$

Ceci vaut de même pour Q. On peut utiliser l'unicité de la factorisation en irréductibles sur l'anneau factoriel $(\mathbb{Z}/p^K\mathbb{Z})[X]$: P coïncide avec un des G_i, H_j **sur** $(\mathbb{Z}/p^K\mathbb{Z})[X]$. Les inégalités sur les coefficients précisées ci-dessus permet de dire que $P \in \{G_1, .., G_s, H_1, ..., H_t\}$. Dès lors, P divise $\text{pgcd}(f,g)$ ou $\text{pgcd}(f,g)$, et donc l'un de ces pgcd est distinct de ± 1.
Notamment, comme on a supposé $\{g,h\} \neq \{f,1\}$, on a que $\text{pgcd}(f,g)$ ou $\text{pgcd}(f,h)$ est non trivial (i.e distinct de ± 1 et de f). □

5.3 Algorithme FACTORISER

Entrées : $f \in \mathbb{Z}[X]$ unitaire et sans facteurs carrés
Sorties : Un couple $g, h \in \mathbb{Z}[X]$ de produit f

Faire
- $R \longleftarrow \mathrm{Res}(f, f')$
- $p \longleftarrow$ Non_Div_Prime(R)
- $(g, h) \longleftarrow$ BERLEKAMP(f, p)
- $n \longleftarrow \deg f$
- $K \longleftarrow \left\lceil \frac{1}{2}\log_p(n+1) + \log_p\left(\binom{n}{\lfloor \frac{n}{2} \rfloor}\right) + \log_p ||f|| \right\rceil$
- $u, v \longleftarrow$ Euclide_Etendu(g, h)
- $i \leftarrow 0$
- **tant que** $2^i \leq 2K$ **faire**
  - $g, h, u, v \longleftarrow$ HENSEL(p, i, f, g, h, u, v)
  - $i \leftarrow i + 1$
- $G \longleftarrow \mathrm{pgcd}(f, g)$
- $H \longleftarrow \mathrm{pgcd}(f, h)$
- **si** $G = 1$ **alors**
  - **Rendre** $(H, f/H)$
- **sinon**
  - **Rendre** $(G, f/G)$

Pseudo-code 5.1 (FACTORISER)**.** *La fonction Euclide_Etendu renvoie les polynômes u, v de la relation de Bézout $ug + vh = 1$.*

6 Correction de FACTORISER

Avant de commenter au sujet de la complexité de FACTORISER, il s'agit de monter la correction.

Déjà, remarquons que le cas $G = H = 1$ n'est jamais atteint. En effet, la démonstration de du lemme 5.5 montre que les deux pgcd ne peuvent pas être simultanément égaux à ± 1.

Nous avons besoin d'un résultat préliminaire :

Lemme 6.1. *Soit* $\mathbf{A}$ *un anneau commutatif quelconque.* $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{A}[X]$ *est inversible si et seulement si* a_0 *est inversible et* $a_1, ..., a_n$ *sont nilpotents.*

Nous admettons ce résultat dans le cadre de ce travail. On en déduit notamment que les inversibles de $\mathbb{Z}[X]$ sont 1 et -1.

Théorème 6.1 (Correction de FACTORISER)**.** *La fonction FACTORISER est correcte, i.e FACTORISER(*f*) renvoie*$(f, 1)$ *si et seulement si* f *est irréductible sur* $\mathbb{Z}[X]$*.*

Démonstration. Soit $f \in \mathbb{Z}[X]$. Quitte à prendre son réduit $\hat{f}$ (lemme 2.4), on suppose f unitaire et sans facteurs carrés.
Supposons que FACTORISER(f) renvoie $(f, 1)$ et montrons alors que f est irréductible sur $\mathbb{Z}[X]$.
Nous avons deux cas : ou bien $(H, f/H) = (f, 1)$ (i.e $f = H$), ou bien $(G, f/G) = (f, 1)$ (i.e $f = G$). Sans perdre de généralité, on suppose que $f = G$. Alors $f = g$ car $G = \text{pgcd}(f, g)$.
On en déduit que la dernière exécution de HENSEL a renvoyé $(f, 1)$. Par l'invariant de boucle du lemme 4.2, nous avons que BERLEKAMP a renvoyé $(f, 1)$. Dès lors, par la correction de BERLEKAMP, f est irréductible sur $\mathbb{F}_p[X]$.
Soit P un facteur irréductible de f. Nous avons alors deux cas : ou bien $P = f \mod p$, ou bien $P = 1 \mod p$ par irréductibilité de f sur $\mathbb{F}_p[X]$. Si $P = f \mod p$, alors nous pouvons appliquer le lemme de Hensel à la factorisation modulo p $f = P \times 1 \mod p$, avec $0 \times P + 1 \times 1 = 1$. En vue des propriétés de la remontée de Hensel, nous avons alors que $f = P \mod p^K$. Par les inégalités sur les coefficients (voir démonstration du lemme 5.5), nous avons donc $f = P$. Donc f est irréductible sur $\mathbb{Z}[X]$.
Réciproquement, si f est irréductible sur $\mathbb{Z}[X]$, alors $\text{pgcd}(f, g) \in \{f, 1\}$. On en déduit donc que FACTORISER(f) renvoie $(f, 1)$.

□

7 Caractérisation des irréductibles de $\mathbb{Z}[X]$

7.1 Énoncé et preuve

Définition 7.1 (Polynôme pseudo-irréductible)**.** *Soit* $f \in \mathbb{Z}[X]$*. Soit un nombre premier* p*. On dira par la suite que* f *est* ***pseudo-irréductible sur*** $\mathbb{F}_p[X]$ *lorsque l'une des deux conditions suivantes est vérifiée :*

1. *$\overline{f}$ est irréductible sur $\mathbb{F}_p[X]$,*
2. *Pour toute factorisation **non triviale** $\overline{f} = \overline{g}\overline{h}$ sur $\mathbb{F}_p[X]$, où $g, h \in \mathbb{Z}[X]$, on a*

$$\left(||g|| > \sqrt{\deg g + 1}\binom{\deg g}{\lfloor \frac{\deg g}{2} \rfloor}||f||\right) \quad \bigvee \quad \left(||h|| > \sqrt{\deg h + 1}\binom{\deg h}{\lfloor \frac{\deg h}{2} \rfloor}||f||\right)$$

où la norme $||.||$ est la norme 2 sur $\mathbb{Z}[X]$, définie au début de la partie 2.3.

Théorème 7.1 (Caractérisation des irréductibles **unitaires** de $\mathbb{Z}[X]$)**.** *Soit $f \in \mathbb{Z}[X]$ unitaire, sans facteurs carrés. Soit p premier ne divisant pas le résultant* $\mathrm{Res}(f, f')$*. Alors f est irréductible sur $\mathbb{Z}[X]$ si et seulement si*

$$\begin{gathered} f \text{ est irréductible sur } \mathbb{F}_p[X], \text{ ou bien} \\ \text{pour toute factorisation } f = gh \text{ sur } \mathbb{F}_p[X], \quad (||g|| > ||f||) \vee (||h|| > ||f||) \end{gathered}$$

où les normes précédentes sont définies par identification des coefficients de g, h à des entiers naturels strictement inférieurs à p.

L'énoncé précédent ne distingue pas f, polynôme de $\mathbb{Z}[X]$, et $\overline{f}$, polynôme de $\mathbb{F}_p[X]$. Par « f est irréductible sur $\mathbb{F}_p[X]$ », nous entendons « la classe $\overline{f}$ d'équivalence modulo p de f est irréductible sur $\mathbb{F}_p[X]$ ». La distinction ne sera pas explicitée par la suite.

Démonstration. Le résultant est non nul puisque l'on suppose f sans facteurs carrés. Le nombre premier p est donc bien défini. Nous avons démontré la correction de FACTORISER. On a la propriété suivante :

> « FACTORISER(f) renvoie la factorisation triviale si et seulement si f est irréductible sur $\mathbb{Z}[X]$ »

De plus, nous avons vu (lemme 4.2) que le couple (G, H) que HENSEL(f, g, h, u, v) renvoie vaut $(f, 1)$ si et seulement si $g = f$ et $h = 1$. Dès lors, f est irréductible si et seulement si BERLEKAMP(f, p) renvoie $(f, 1)$. □

Exemple. Prenons $f = X^4 + 1$, polynôme unitaire et sans facteurs carrés. On a $f' = 4X^3$. La matrice de Sylvester associée est :

$$S_f = \begin{pmatrix} 1 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}_{(7)}$$

Les racines de f' sont $0, 0, 0$ d'où, par le théorème 2.3 :

$$\begin{aligned}\det S_f &= (-1)^{3\times 4} 4^4 \prod_{j=1}^{3} f(0) \\ &= 4^4 \prod_{j=1}^{3} (+1) \\ &= 4^4 = 256\end{aligned}$$

Les racines complexes de f sont, en notant $\zeta := e^{\frac{i\pi}{4}}$,

$$\zeta, \quad \zeta^3, \quad \zeta^5, \quad \zeta^7$$

On en déduit par le théorème 2.3 que :

$$\begin{aligned}\det S_f &= \prod_{k=0}^{3} 4 \left(\zeta^{2k+1}\right)^3 \\ &= 4^4 \exp\left(\frac{3i\pi}{4} + \frac{9i\pi}{4} + \frac{15i\pi}{4} + \frac{21i\pi}{4}\right) \\ &= 256 \exp\left(\frac{48i\pi}{4}\right) \\ &= 256\end{aligned}$$

On obtient le même résultat pour les deux calculs. Notamment :

$$5 \text{ est un nombre premier ne divisant pas } \mathrm{Res}(f, f')$$

Étudions alors l'irréductibilité de f dans $\mathbb{F}_5[X]$. Procédons par le lemme de Berlekamp (théorème 3.1). On a, modulo f,

$$\begin{aligned}X^{5\times 0} - X^0 &\equiv 0 \\ X^{5\times 1} - X^1 &\equiv -2X \\ X^{5\times 2} - X^2 &\equiv 0 \\ X^{5\times 3} - X^3 &\equiv -2X^3\end{aligned}$$

d'où la matrice de l'endomorphisme de l'algèbre-quotient $\mathbb{F}_5[X]/(f)$ $S : a \mapsto a^4 - a$ dans la base $(1, X, X^2, X^3)$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

donc X^2 est dans l'algèbre de Berlekamp $\ker S$ et n'est pas constant. On en déduit donc que f n'est pas irréductible sur $\mathbb{F}_5[X]$: on a

$$f = (X^2 + 2)(X^2 - 2)$$

Appliquons cependant le lemme de Hensel à la factorisation de f. On a la relation de Bézout dans $\mathbb{F}_5[X]$: $1 \times (X^2-2) + (-1) \times (X^2+2) = 1$. On obtient successivement :

1. $\text{HENSEL}(f, X^2-2, X^2+2, 1, -1) \longrightarrow X^2-7, X^2+7, 16, -16$
2. $\text{HENSEL}(f, X^2-7, X^2+7, 16, -16) \longrightarrow X^2-807, X^2+807,$

Théorème 7.2 (Caractérisation des polynômes de $\mathbb{Z}[X]$ irréductibles sur $\mathbb{Q}[X]$)**.** *Soit $f \in \mathbb{Z}[X]$ sans facteurs carrés. On note $\hat{f}$ le réduit de f défini au lemme 2.4. Soit p premier ne divisant par $\text{Res}(\hat{f}, \hat{f}')$. f est irréductible sur $\mathbb{Q}[X]$ si et seulement si $\hat{f}$ est irréductible sur $\mathbb{F}_p[X]$.*

Démonstration. Le lemme 2.5 affirme que f est irréductible sur $\mathbb{Q}[X]$ si et seulement si $\hat{f}$ l'est. Or $\hat{f}$ est unitaire, et donc primitif : par le lemme 2.3, f est irréductible sur $\mathbb{Q}[X]$ si et seulement si $\hat{f}$ est irréductible sur $\mathbb{Z}[X]$. De plus, par le lemme 2.8, on a que $\hat{f}$ est sans facteurs carrés. Par le théorème précédent appliqué à $\hat{f}$ qui est unitaire et sans facteurs carrés, $\hat{f}$ est irréductible sur $\mathbb{Z}[X]$ si et seulement si $\hat{f}$ est irréductible sur $\mathbb{F}_p[X]$. □

7.2 Exemples d'application

7.2.1 Le critère d'Eisenstein

Théorème 7.3 (Critère d'Eisenstein)**.** *Soit $f = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :*

1. *p divise $a_0, a_1, ..., a_{n-1}$.*
2. *p ne divise pas a_n.*
3. *p^2 ne divise pas a_0.*

Alors f est irréductible sur $\mathbb{Q}[X]$.

Démonstration « classique ». Supposons que f ne soit pas irréductible sur $\mathbb{Q}[X]$. Par le lemme 2.5, on peut prendre le réduit $\hat{f}$ de f. Par définition, on a

$$\hat{f} = \sum_{k=0}^{n} a_k a_n^{n-1-k} X^k$$

ce qui maintient les hypothèses du critère d'Eisenstein. De plus, $\hat{f}$ est dorénavant primitif et non irréductible sur $\mathbb{Q}[X]$, donc par le lemme 2.3, $\hat{f}$ est non irréductible sur $\mathbb{Z}[X]$. Il existe donc $g, h \in \mathbb{Z}[X]$ non inversibles dans $\mathbb{Z}[X]$ tels que $f = gh$. Modulo p, on a donc

$$X^n = g \times h \mod p$$

Or les diviseurs de X^n dans $\mathbb{F}_p[X]$ sont les X^i, $i \in \{0, ..., n\}$, donc

$$g = X^r \mod p, \quad h = X^s \mod p$$

où $r + s = n$. On note b_0, c_0 les coefficients constants respectifs de g, h, et on déduit que $b_0 = c_0 = 0 \mod p$. Dès lors, $p | b_0$, et $p | c_0$, donc $p^2 | b_0 c_0 = a_0 a_n^{n-1}$. Absurde !

Donc f est irréductible sur $\mathbb{Q}[X]$. □

Remarque 7.1. On n'aurait pas pu appliquer ici la caractérisation 7.2. En effet, le résultant $\mathrm{Res}(\hat{f}, \hat{f}')$ est nul modulo p, puisque la dernière ligne de la matrice de Sylvester associée est nulle modulo p. Dès lors, notre caractérisation ne sert pas dans ce cadre.

7.2.2 Application aux polynômes cyclotomiques

Définition 7.2 (n-ième polynôme cyclotomique)**.** *Soit $n \in \mathbb{N}^*$. On appelle **n-ième polynôme cyclotomique** le polynôme Φ_n défini par :*

$$\Phi_n \quad := \quad \prod_{k=0, \mathrm{pgcd}(k,n)=1}^{n-1} (X - \exp\frac{2ik\pi}{n})$$

*Pour simplifier les notations, on dira qu'une racine n-ième de l'unité z est **primitive** lorsque $z^d \neq 1$ pour tout entier $d > 0$ divisant n. On note $\mathbb{P}_n$ l'ensemble des racines primitives n-ièmes de l'unité. On pourra alors écrire*

$$\Phi_n = \prod_{z \in \mathbb{P}_n} (X - z)$$

Lemme 7.1. *Pour tout $n \geq 1$, on a*

$$X^n - 1 = \prod_{d|n} \Phi_d$$

le produit étant prit sur l'ensemble des entiers $d > 0$ divisant n.

Démonstration. On procède par égalité des racines comptées avec multiplicité. Soit z une racine de $X^n - 1$. Alors z est racine simple de $X^n - 1$, et il existe $d > 0$ divisant n tel que $z^d = 1$. On prend d minimal. Alors z est racine simple de Φ_d. De plus, pour tout $d' > 0$ divisant n, si z est une racine de $\Phi_{d'}$ alors $z \in \mathbb{P}_{d'}$, ce qui implique $d = d'$ par minimalité de d. Donc z est racine simple du produit.

Réciproquement, toute racine du produit est racine de $X^n - 1$.

On a ainsi égalité des racines. Les deux polynômes étant unitaires, (car les Φ_d le sont), on a égalité des polynômes. □

Remarque 7.2. La démonstration précédente offre une démonstration originale de l'identité

$$n = \sum_{d|n} \phi(d)$$

où ϕ est l'indicatrice d'Euler définie pour tout entier $n \geq 1$ par

$$\phi(n) = \mathrm{Card}\ \{0 \leq k < n; \mathrm{pgcd}(k, n) = 1\}$$

En effet, Φ_d est de degré $\phi(d)$, et on conclut par égalité des degrés.

Lemme 7.2. *Soit p un nombre premier, et $k \geq 1$ un entier. On a*

$$\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + ... + X^{p^{k-1}} + 1$$

Démonstration. On a :

$$\begin{aligned} X^{p^k} - 1 = \prod_{0 \leq j \leq k} \Phi_{p^j} &= \Phi_{p^k} \times \prod_{0 \leq j < k} \Phi_{p^j} \\ &= \Phi_{p^k} \times (X^{p^{k-1}} - 1) \end{aligned}$$

Donc

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \frac{(X^{p^{k-1}} - 1)(X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + ... + X^{p^{k-1}} + 1)}{X^{p^{k-1}} - 1}$$

D'où le résultat. □

Exemple. Les six premiers polynômes cyclotomiques sont :

$$\Phi_1 = X - 1$$

$$\Phi_2 = X + 1$$

$$\Phi_3 = X^2 + X + 1$$

$$\Phi_4 = X^2 + 1$$

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1$$

$$\Phi_6 = X^2 - X - 1$$

On conjecture donc que $\Phi_n \in \mathbb{Z}[X]$ pour tout $n \geq 1$.

Lemme 7.3. *Pour $n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$.*

Démonstration. On raisonne par récurrence forte sur n.
Initialisation On a bien $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.
Hérédité On suppose que la propriété est vérifiée pour tout $1 \leq k \leq n-1$, où $n \geq 2$. Le polynôme $A := \prod_{d|n, d<n} \Phi_d := \sum_{i=0}^{r} a_r X^r$ est donc à coefficients entiers. Notons

$$\Phi_n = \sum_{i=0}^{+\infty} p_i X^i$$

Alors l'identité $X^n - 1 = \Phi_n \times A$ implique que :

$$\forall j \geq r, \quad \sum_{i=0}^{r} a_i p_{j-i} \in \mathbb{Z}$$

Ce que l'on note en introduisant des entiers c_j :

$$\forall j \geq r, \quad p_{j-r} = -\sum_{i=0}^{r-1} a_i p_{j-i} + c_j$$

Or les a_i sont entiers et les p_i sont nuls à partir d'un certain rang. Par une récurrence descendante, on obtient donc que $p_{j-r} \in \mathbb{Z}$ pour tout $j \geq r$. Donc $\Phi_n \in \mathbb{Z}[X]$.

On conclut par le principe de récurrence. □

Lemme 7.4. *Soit p un nombre premier. Soit $k \in \mathbb{N}$. Alors Φ_{p^k} est irréductible dans $\mathbb{Z}[X]$.*

Démonstration. La matrice de Sylvester associée à Φ_{p^k} et Φ'_{p^k} est :

$$S_p := \begin{pmatrix} 1 & 0 & - & 0 & (p-1)p^{k-1} & 0 & - & 0 \\ 0 & 1 & - & 0 & 0 & (p-1)p^{k-1} & - & 0 \\ 0 & 0 & - & 0 & 0 & 0 & - & 0 \\ | & | & & | & | & | & & 0 \\ 1 & 0 & - & 1 & 0 & 0 & - & (p-1)p^{k-1} \\ 0 & 1 & - & 0 & p^{k-1} & 0 & - & 0 \\ | & | & & | & | & | & & | \\ 0 & 0 & - & 1 & 0 & 0 & - & p^{k-1} \end{pmatrix}$$

En retirant $(p-1)p^{k-1}$ fois la première colonne à la □

8 Bestiaire de fonctions OCaml

8.1 Complexité

8.2 Représentations de polynômes en OCaml

L'implémentation se fait, dans le cadre de ce travail, en OCaml. Afin de distinguer le code du français et des mathématiques, le texte sera écrit en **gras** lorsqu'il s'agit d'un élément de OCaml. Un polynôme de $\mathbb{Z}[X]$ sera représenté par le type :

```
type polynome = {mutable deg : int ; coefs : int array};;
```

Définition 8.1. *Si* ***p : polynome*** *est un polynôme ainsi défini, représentant* $P = \sum_{i=0}^{n} p_i X_i$*, alors* ***p.coefs*** *est un tableau d'au moins* $n+1$ *cases représentant les coefficients de* P*. On a, pour tout* $i \in \{0, ..., n\}$*,* ***p.coefs.(i)*** $= p_i$*, et* ***p.deg*** $= n$*. Ainsi, nous ferons l'hypothèse de toujours avoir que* ***p.coefs.(n)*** *est nul si et seulement si* $P = 0$*.*

Cette hypothèse ne sera en fait pas toujours vérifiée dans notre implémentation, notamment au sein de certaines fonctions. Par exemple, pour la division euclidienne (8.5), nous ne nous préoccuperons pas de la conservation de cette hypothèse pour le polynôme reste **r**.

On introduit de plus le type *opérateur*, qui représentera des fonctions de sommation $+$, ou de produit $\times$. L'introduction d'un tel opérateur permettra de conserver la généralité des opérateurs algébriques (tels **somme** ou **prod**), sans avoir besoin de modifier la fonction lorsqu'on travaille dans l'anneau $\mathbb{Z}[X]$ ou dans l'anneau $\mathbb{F}_p[X]$.

```
type op = int->int->int;;
```

Dans le cadre du produit de polynômes, nous effectuerons une séquence de produit de monômes par un polynôme :

$$(a_0 + a_1 X + ...a_n X^n)B \quad = \quad (a_0 X^0)B + (a_1 X)B + ... + (a_n X^n)B$$

On implémente donc le type **monome** qui permet de représenter et de manipuler de façon plus efficace les monômes :

```
type monome = {deg : int ; coef : int};;
```

8.3 Premières opérations sur les polynômes

Initialisateurs

On introduit les initialisateurs suivants, qui s'effectuent en temps borné :

```
let polynome_nul () = { deg = -1 ; coefs = [|0|] };;
let monome_nul () = { deg = -1 ; coef = 0 };;

let init_monome (coef:int) (degre:int) =
```

```
    match coef with
    | 0 -> monome_nul ()
    | n -> { deg  = n ; coef = coef};;
```

ainsi que les initialisateurs suivants, qui s'effectuent en temps linéaire en les paramètres d'entrée :

```
let init_polynome (a:int array) =
    match a with
    | [||] -> polynome_nul ()
    | t -> {deg = Array.length t - 1; coefs = a};;
let copie (a:polynome) =
    match a.deg with
    | -1 -> { deg = -1 ; coefs = [||] }
    | n -> let f (i:int) = a.coefs.(i) in
           { deg = n ; coefs = Array.init (n+1) f };;

let convert_monome (a:monome) =
    match a.deg with
    | -1 -> polynome_nul()
    | n -> (let t = Array.make (n+1) 0 in
            t.(n) <- a.coef;
            {deg = n ; coefs = t} );;
```

Accesseurs
On introduit les accesseurs suivants, qui s'effectuent en temps borné :

```
    let est_nul (a:polynome) = (a.deg = -1);;
    let deg (p:polynome) = p.deg;;
    let coefs (p:polynome) = p.coefs;;
    let coef_dominant (p:polynome) = match p.deg with
    | -1 -> 0
    | n -> p.coefs.(n);;
```

On introduit de plus l'accesseur **liste_monomes**, qui s'effectue en temps linéaire en le degré du polynôme fourni :

```
let liste_monomes (a:polynome) =
    let rec aux (a:polynome) =
        match a.deg with
        | -1 -> []
        | n when a.coefs.(n) <> 0 ->
            ( a.deg <- (n-1) ;
            {deg = n ; coef = a.coefs.(n)}::(aux a) )
        | n -> (a.deg <- (n-1) ; aux a )
    in let n = a.deg
    in let r = aux a
    in a.deg <- n ; r;;
```

Cette fonction renvoie une représentation du polynôme en une liste (ordonnée en degré) de monômes. On a ainsi une fonction permettant de changer de représentation d'un polynôme.

Mutateurs
On introduit le mutateur **mult_scalaire** qui multiplie chacun des coefficients de **a** par **x**, pour l'opérateur algébrique (sur $\mathbb{Z}$) **pr** :

```
let mult_scalaire (a:polynome) (x:int) (pr:op) =
    match a.deg with
    | -1 -> ()
    | n -> (for i=0 to n do
                a.coefs.(i) <- pr x a.coefs.(i)
            done);;
let mod_p_polynome (a:polynome) (p:int) =
    if p=0 then
        failwith "Division par 0";
    let mod_p (x:int) (p:int) = x mod p
    in mult_scalaire a p mod_p;;
```

La deuxième fonction introduite ci-dessus permet de "réduire" le polynôme **a** modulo un entier p fourni.

8.4 Opérateurs algébriques

Dans cette partie, **A** désigne un des anneaux $\mathbb{Z}$ ou $\mathbb{Z}/p^k\mathbb{Z}$.

8.4.1 Somme de polynômes

On définit l'opérateur somme + sur $\mathbf{A}[X]$ par la fonction suivante :

```
let somme (p:polynome) (q:polynome) (ad: int->int->int) =
    let n = p.deg in
    let m = q.deg in
    let d = ref (max n m) in
    (* calcul du degré de la somme lorsque les degrés sont égaux *)
    if n=m then (
        while ( ad q.coefs.(!d) p.coefs.(!d) = 0) && ( !d <> 0 ) do
            d := !d - 1
        done;
    );
    let s = {deg = !d ; coefs = Array.make (!d+1) 0} in
    for i=0 to !d do
        if i<=n then (
            s.coefs.(i) <- p.coefs.(i)
        );
        if i<=m then (
            s.coefs.(i) <- ad s.coefs.(i) q.coefs.(i)
```

```
    )
done; s;;
```

La fonction précédente prend en entrée un deux polynômes **a** et **b**, ainsi qu'une fonction d'addition **ad**. Préciser la fonction d'addition permet notamment de calculer des polynômes modulo p^k. On suppose que la fonction **ad** a une complexité bornée (à lire : en $O(1)$).

Étude de complexité 1. *La complexité d'un appel à* ***somme a b ad*** *est en* $O(\max(\textbf{\textit{a.deg}}, \textbf{\textit{b.deg}}))$.

Démonstration. La boucle **while** boucle au plus $n := \max(\textbf{a.deg}, \textbf{b.deg})$ fois. Chaque itération effectue une opération bornée en complexité. La boucle **for** boucle n fois, effectuant à chaque fois au plus quatre opérations toutes bornées en temps (par l'hypothèse sur **ad** précisée précédemment). En somme, on a une complexité en $O(n)$. □

8.4.2 Produit de polynômes

On introduit l'opérateur produit $\times$ sur $\mathbf{A}[X]$ par la fonction suivante :

```
let prod (a:polynome) (b:polynome) (ad:op) (pr:op) =
match a.deg, b.deg with
| -1, _ -> polynome_nul ()
| _, -1 -> polynome_nul ()
| n,m ->begin
    (* initialisation du polynôme produit *)
    let t = Array.make (n+m+1) 0 in
    (* calcul récursif des coefficients par la liste des monômes *)
    let rec prod_aux (l:monome list) =
    match l with
    | [] -> ()
    | hd::tl -> (
        for i=0 to m do
            t.(hd.deg+i) <- ad t.(hd.deg+i) (pr hd.coef b.coefs.(i))
        done )
    in prod_aux (liste_monomes a);
    { deg = n+m ; coefs = t };
    end;;
```

La fonction précédente prend en entrée une fonction produit **pr** supplémentaire, pour les mêmes raisons que la fonction d'addition **ad** : c'est-à-dire calculer dans $\mathbb{Z}/p^k\mathbb{Z}$. On supposera dans toute la suite qu'un appel à **pr** se fait en temps constant (à lire : en $O(1)$). Le fonctionnement est le suivant : on décompose **a** en sa liste de monômes. On initialise ensuite le tableau **t** représentant le polynôme produit, et à chaque monôme **hd** de **a**, on modifie les coefficients de **t**. Cette modification se fait par l'association, pour tout $i \in \{0, ..., \textbf{b.deg}\}$:

$$t_{n+i} := a_n \times b_i$$

Étude de complexité 2. *La complexité d'un appel à* ***prod a b ad pr*** *est en* $O(\textbf{\textit{a.deg}} \times \textbf{\textit{b.deg}})$.

Démonstration. L'appel à **liste_monomes a** se fait en $O(\textbf{a.deg})$. L'initialisation de **t** se fait en un $O(\textbf{a.deg} + \textbf{b.deg})$. Le traitement d'un monôme se fait en un $O(\textbf{b.deg})$, car le contenu de la boule **for** se fait en temps borné. Dès lors, la complexité est en $O(\textbf{List.length (liste\_monomes a)} \times \textbf{b.deg})$, i.e, le nombre de coefficients non nuls de **a** multiplié par le degré de **b**. Par la suite, on utilisera la complexité $O(\textbf{a.deg} \times \textbf{b.deg})$. □

8.5 Division euclidienne de polynômes

On introduit la division euclidienne par :

```
let div_euc (a:polynome) (b:polynome) (ad:op) (pr:op) =
    if b.deg = -1 then
        failwith "Division par zéro";
    let r = copie a in
    let delta = deg a - deg b in
    if delta >= 0 then begin
        (* initialisation du quotient *)
        let q = {deg = delta ; coefs = Array.make (delta+1) 0} in
        while deg r >= deg b do
            let alpha = coef_dominant r / coef_dominant b in
            let d = deg r - deg b in
            q.coefs.(d) <- alpha;
            (* on retire à R le produit alpha * X^d * B *)
            for i=0 to (deg b) do
                r.coefs.(d+i) <- ad r.coefs.(d+i) (pr (pr (-1) alpha) b.coefs.(i) )
            done ;
            r.deg <- r.deg - 1
        done ; (q, r);
    end
    else
        (polynome_nul (), copie a);;
```

Étude de complexité 3. *La complexité d'un appel à* ***div_euc a b ad pr*** *se fait en* $O(\textbf{\textit{b.deg}} \times (\textbf{\textit{a.deg}} - \textbf{\textit{b.deg}} + 1))$.

Démonstration. Les définitions se font en temps linéaire en le degré de **a** à cause de **copie a**. L'initialisation de **q** se fait en $O(\delta + 1)$, où $\delta = \textbf{a.deg} - \textbf{b.deg}$. On itère δ fois un traitement s'effectuant en un $O(\textbf{b.deg})$ (boucle **for** itérant des opérations en temps borné). En somme, on obtient une complexité en

$$O(\textbf{a.deg} + (\delta + 1) \times (\textbf{b.deg} + 1)) = O(\textbf{b.deg} \times (\delta + 1))$$

□

8.6 Pivot de Gauss

Soit S une matrice de taille $n \times m$ à coefficients dans $\mathbb{Z}$. On introduit des fonctions préliminaires. Les complexités sont en $O(m)$, sauf pour **div_scal**, dont la complexité est en $O(n \times m)$.

```
type matrix = int array array;;

(* échange de deux lignes *)
let echange_lignes (s:matrix) (i:int) (l:int) =
    let t = Array.copy s.(i) in
    s.(i) <- Array.copy s.(l) ;
    s.(l) <- t;;

(* multiplication d'une ligne par un scalaire *)
let mult_scal (s:matrix) (i:int) (x:int) =
    let m = Array.length s.(i) in
    for j=0 to (m-1) do
        s.(i).(j) <- x * s.(i).(j);
    done;;

(* On multiplie toutes les autres lignes par x,
   ce qui permet de rester dans M_n(Z) *)
let div_scal (s:matrix) (i:int) (x:int) =
    let n = Array.length s in
    let m = Array.length s.(i) in
    for l=0 to (n-1) do
        if l<>i then (
            for j=0 to (m-1) do
                s.(l).(j) <- x * s.(l).(j)
            done;
        )
    done;;

(* effectue L_i <- x * L_l + L_i *)
let ajout (s:matrix) (i:int) (l:int) (x:int) =
    let m = Array.length s.(i) in
    for j=0 to (m-1) do
        s.(i).(j) <- s.(i).(j) + x * s.(l).(j)
    done;;
```

On peut alors procéder à l'implémentation de l'algorithme de *Gauss-Jordan* pour réduire la matrice S.

```
let gauss_jordan (s:matrix) =
    let n = Array.length s -1 in
    let m = Array.length s.(0) -1 in
    (* repère le pivot précédent *)
    let r = ref (-1) in
    for j=0 to m do
        (* recherche du prochain pivot *)
        let i0 = ref (!r +1) in
        for i = (!r + 1) to n do
            if abs s.(i).(j) > abs s.(!i0).(j) then
                i0 := i
        done ;
        let k = !i0 in
        if s.(k).(j) <> 0 then begin
            r := !r + 1;
            div_scal s k s.(k).(j);
            if k <> !r then
                echange_lignes s k !r;
            for i=0 to n do
                if i <> !r then
                    ajout s i !r (- s.(i).(j) / s.(!r).(j))
            done;
        end;
    done;;
```

Une fois la matrice réduite, on peut extraire un vecteur du noyau :

```
let vecteur_ker (s:matrix) =
    gauss_jordan s;
    let n = Array.length s in
    let v = Array.make n 0 in
    (* Pour le système Sv=0, v.(n-1) est toujours nul *)
    for i=1 to (n-1) do
        if s.(n-1-i).(n-1-i) <> 0 then
            v.(n-1-i) <-
                ( let sigma = ref 0 in
                   for j=(n-i) to (n-1) do
                       sigma := !sigma - s.(n-1-i).(j) * v.(j) ;
                       v.(j) <- v.(j) * s.(n-1-i).(n-1-i)
                    done; !sigma )
        else
            v.(n-1-i) <- 1;
    done; v;;
```

La définition précédente admet une propriété intéressante :

Lemme 8.1. *L'appel* ***vecteur_ker s*** *renvoie le vecteur nul si et seulement si* ***s*** *est inversible.*

Démonstration. **s** est inversible si et seulement si sa réduite de Gauss-Jordan l'est. En admettant la correction de l'algorithme, cela est analogue à dire que la réduite de Gauss-Jordan de **s** n'a aucun coefficient diagonal nul.

Supposons que la réduite de Gauss-Jordan de **s** admette un coefficient diagonal nul, i.e que **s** est non inversible. Dès lors, s'il s'agit du i^e coefficient diagonal, on a **v.(i) = 1** avant multiplication possible par un scalaire non nul et réduction. Donc le vecteur **v** renvoyé est non nul.

Réciproquement, supposons que la réduite de Gauss-Jordan de **s** n'admette pas de coefficient diagonal nul, i.e que **s** est inversible. Dans ce cas, on peut invoquer l'invariant de boucle « ***v.(i)*** *est nul si tous les* ***v.(j)****,* $j > i$ *sont nuls* ». Celui-ci est immédiat puisque la condition **s.(n-1-i).(n-1-i) <> 0** est toujours vérifiée. Dès lors, sachant que **v.(n-1)** est nul, on a par récurrence que **v** est le vecteur nul. □

Passons à la complexité.

Étude de complexité 4 (Pivot de Gauss)**.** *La complexité d'un appel à* ***vecteur_ker s****, où* ***s*** *est une matrice carrée de taille* n*, est en* $O(n^3)$*.*

Démonstration. Mis à part l'appel **gauss_jordan s**, le reste de la fonction **vecteur_ker s** a une complexité en $O(n^2)$. Le gros de la complexité vient donc de la réduite de Gauss-Jordan. On boucle $m = n$ fois :

1. la recherche d'un maximum dans un ensemble de n éléments ($O(n)$),
2. la division par un scalaire de la matrice, par **div_scal**, qui a une complexité en $O(n \times m)$,
3. une boucle qui appelle **ajout** n fois : $O(n \times m)$.

On a donc une complexité en

$$O(m[n + n \times m + n \times m]) = O(n \times m^2) = O(n^3)$$

□

8.7 Calcul de la matrice S

8.8 Représentation de factorisations dans $\mathbb{Z}/p^k\mathbb{Z}$

On définit de plus une *factorisation* d'un polynôme de $\mathbb{Z}[X]$ par le type :

```
type fact = {a : polynome ;
             p : int ;
             k : int ;
             mutable facteurs : polynome list};;
```

Soit **f :fact**, et soit $P \in \mathbb{Z}[X]$. On dira que **f** est une *factorisation de degré* k de P lorsque :

1. **f.p** est un nombre premier.

2. **f.facteurs** est une factorisation de P modulo $\mathbf{f.p}^{\mathbf{f.k}}$ en polynômes unitaires et premiers entre eux deux à deux. Autrement dit, si **f.facteurs** $= [f_1; ...; f_r]$, alors $f_1, ..., f_r$ sont unitaires premiers entre eux deux à deux, et :

$$P \quad \equiv \quad \mathbf{f.a} \quad \equiv \quad f_1 f_2 ... f_r \mod \mathbf{f.p}^{\mathbf{f.k}} \tag{6}$$

En pratique, **f.k** sera une puissance de 2. Le lemme de Hensel passera donc d'une factorisation de degré k de P à une factorisation de degré $2k$ de P. La première factorisation sera donnée par l'algorithme de Berlekamp.

8.9 Algorithme de Berlekamp

L'objectif de cette partie est de définir une fonction OCaml :

```
berlekamp : polynome -> int -> fact
```

qui s'appuie sur le pseudo-code 3.1 (Berlekamp).

9 Sources

1. ABUAF ROLAND, BOYER IVAN : *Factorisation dans Z[X] : Sujet de maîtrise proposé par François Loeser*, 2007
2. GOTTHOLD EISENSTEIN : Eisenstein, zur Lemniscatentheilung : *Journal für die reine und angewandte Mathematik*, 1850, 160-179
3. ELWYN R. BERLEKAMP : Factoring Polynomials Over Finite Fields : Bell Systems Technical Journal, 1967, 46 :1853-1859
4. RAY MINES, FRED RICHMAN et WIM RUITENBURG, *A Course in Constructive Algebra*, Springer, p. 123.
5. M WEIMANN : Factorisation dans Z[X] : *UFR Sciences, M2 Calcul Formel, Option Maths approfondies* (2012)
6. MOHAMED NASSIRI, *Critère d'Eisenstein*, Coquillages&Poincaré, agreg-maths.fr, [en ligne], consulté en mai 2025