INFORMATIQUE THÉORIQUE ET APPLICATIONS

GUY VIRY

Factorisation sur $\mathbb{Z}[X]$ des polynômes de degré élevé à l'aide d'un monomorphisme

Informatique théorique et applications, tome 24, n° 4 (1990), p. 387-407

<http://www.numdam.org/item?id=ITA_1990__24_4_387_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 24, n° 4, 1990, p. 387 à 407)

FACTORISATION SUR $\mathbb{Z}[X]$ DES POLYNÔMES DE DEGRÉ ÉLEVÉ À L'AIDE D'UN MONOMORPHISME (*)

par Guy VIRY (1)

Communiqué par J. BERSTEL

Résumé. – *Le but de cet article est d'améliorer un algorithme défini dans* [7]. *Cet algorithme utilise un monomorphisme qui transforme tout produit en somme. Grâce à ce monomorphisme on obtient un critère améliorant la recherche des diviseurs d'un polynôme de* $\mathbb{Z}[X]$ *à partir de ses diviseurs sur* $\mathbb{Z}/(p^m)[X]$.

Notons P le polynôme donné de $\mathbb{Z}[X]$, *d son degré et r le nombre de ses facteurs sur* $\mathbb{Z}/(p)[X]$. *Dans l'algorithme usuel, défini par Wang dans* [8], *le coût est dominé par le calcul de* 2^r *produits de polynômes, ce qui donne* $2^r d^2 (d + \mathrm{Log} \| a_0 P \|)^2$.

Avec le nouvel algorithme, le facteur $(d + \mathrm{Log} \| a_0 P \|)^2$ *est remplacé par* $2 + Log \| P \|$. *Mais, comme les calculs doivent être effectués modulo un nombre* p^m *supérieur à* $(4 \| P \|)^d$, *le coût n'est meilleur que si d est suffisamment grand, par rapport à* $\| P \|$.

Abstract. – *We improve an algorithm that is defined in* [7]. *This algorithm uses a monomorphism that transforms any product into a sum. Thanks to this monomorphism we get a method of searching the factors of a polynomial of* $\mathbb{Z}[X]$, *from its factors over* $Z/(p^m)[X]$. *We denote by P the given polynomial of* $\mathbb{Z}[X]$, *by d its degree and by r the number of its factors over* $\mathbb{Z}/(p)[X]$.

In the usual algorithm, defined by Wang in [8], *the complexity is dominated by the computation of* 2^r *products of polynomials that is bounded by* $2^r d^2 (d + \mathrm{Log} \| a_0 P \|)^2$.

With the new algorithm the factor $(d + \mathrm{Log} \| a_0 P \|)^2$ *is replaced by* $2 + \mathrm{Log} \| P \|$. *But the use of the monomorphism increases the complexity of the preceeding step of the algorithm, because the computation must be made modulo a number greater than* $(4 \| P \|)^d$. *On the whole, the complexity of the new algorithm is better, only if the degree of P is sufficiently large, in comparison with* $\| P \|$.

INTRODUCTION

On se propose d'utiliser un monomorphisme Φ_n qui transforme un produit en une somme, afin d'améliorer l'algorithme classique de factorisation sur $\mathbb{Z}[X]$. On reprend en l'améliorant un algorithme défini dans [7].

(*) Reçu en juillet 1988, révisé en février 1989.
(1) Département de Mathématiques, B.P. n° 10662, Université de Niamey, Niamey, Niger.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/90/04 387 21/$4.10/

On adopte dans tout l'article les notations suivantes pour les logarithmes : Log désigne le logarithme dans la base 2 et Ln le logarithme népérien.
Dans la suite, on note $P = a_0 X^d + \ldots + a_{d-1} X + a_d$ un polynôme de $\mathbb{Z}[X]$ sans facteur carré; on peut toujours se ramener à ce cas en divisant P par le PGCD de P et P'.

La méthode classique de factorisation est définie par Wang et Rothschield dans [8]. Elle consiste à choisir un entier premier p tel que P reste sans facteur carré sur $\mathbb{Z}/(p)$. Ensuite P est factorisé sur $\mathbb{Z}/(p)$ à l'aide de l'algorithme de Berlekamp. On en déduit, grâce au lemme de Hensel, la factorisation de P sur $\mathbb{Z}/(p^m)[X]$ où p^m majore les coefficients des diviseurs de P sur $\mathbb{Z}[X]$. Notons $Q_1 \ldots Q_j \ldots Q_r$ la factorisation de P sur $\mathbb{Z}/(p^m)[X]$. Ensuite on doit calculer tous les sous-produits de $Q_1 \ldots Q_j \ldots Q_r$ pour vérifier si l'un d'eux divise P sur $\mathbb{Z}[X]$. Si ce n'est pas le cas, alors P est irréductible.

La méthode proposée ci-dessous consiste à calculer les images des facteurs Q_j de P par Φ_n. La recherche des sous-produits de $Q_1 \ldots Q_r$ de l'algorithme classique est remplacée ici par la recherche des sous-sommes de $\Phi_n(Q_1) + \ldots + \Phi_n(Q_r)$. On obtient ainsi un critère de reconnaissance des diviseurs de P sur $\mathbb{Z}[X]$.

Dans la méthode classique, le coût est dominé par le calcul des sous-produits de

$$Q_1 \ldots Q_j \ldots Q_r \quad \text{sur } \mathbb{Z}/(p^m)[X] \qquad \text{avec } p^m > 2^d |a_0| . \| P \|.$$

Comme il y a 2^{r-1} produits à calculer, ainsi que 2^{r-1} divisions, le coût est donné par

$$2^r d^2 (d + \text{Log} \| a_0 P \|)^2.$$

Le coût est donc exponentiel. Mais le nombre r est « en général » très petit devant d, bien que sa borne théorique reste d.

Berlekamp signale dans [1], page 86, que pour d « suffisamment grand », une valeur approximative de r est donnée par $\text{Ln}(d)$. Un résultat précis est donné par M. Mignotte et J. L. Nicolas dans [4]. Ce résultat sera analysé dans le paragraphe IV et il permet par exemple d'affirmer qu'un polynôme quelconque de $\mathbb{Z}/(p)[X]$ a au moins une chance sur deux de vérifier

$$|r - \text{Ln}(d)| < \sqrt{8 \text{ Ln } (d)}.$$

Avec cette approximation, on obtient un coût usuel égal à

$$d^{2 + 2.\text{Ln}(2)} (d + \text{Log} \| a_0 P \|)^2. \tag{I}$$

Avec la méthode proposée le facteur $(d+\mathrm{Log}\,\|a_0 P\|)^2$ est remplacé par $2+\mathrm{Log}\,\|P\|$. Mais l'utilisation du monomorphisme Φ_n augmente les calculs de la factorisation sur $\mathbb{Z}/(p^m)[X]$, car les calculs doivent être faits modulo p^m avec

$$p^m > (4\,\|P\|)^d.$$

Mais au total le coût du nouvel algorithme est meilleur que celui de l'algorithme classique, si on choisit le degré d de P suffisamment grand, par rapport à $\|P\|$.

Signalons aussi la méthode proposée par Lenstra dans [3]. Les calculs sont de l'ordre de $d^{12}\,\mathrm{Log}^2\,\|a_0 P\|$. Le coût n'est donc plus exponentiel comme dans l'algorithme classique, mais il est nettement supérieur au coût usuel donné ci-dessus en (I).

I. DÉFINITION DU MONOMORPHISME Φ_n

Considérons le polynôme suivant de $\mathbb{Z}[X]$:

$$P(X) = a_0 X^d + a_1 X^{d-1} + \ldots + a_{d-1} X + a_d,$$

dont les coefficients $a_0, a_1, \ldots, a_d$ sont premiers entre eux; un tel polynôme est appelé polynôme primitif.

Remarquons qu'on peut facilement transformer P en polynôme unitaire, en remplaçant X par X/a_0 dans P, puis en multipliant l'expression obtenue par a_0^{d-1}; on obtient le polynôme :

$$\begin{aligned} P_u(X) &= a_0^{d-1} P(X/a_0) \\ &= X^d + a_1 X^{d-1} + a_2 . a_0 X^{d-2} + \ldots + a_d . a_0^{d-1}. \\ &= X^d + \alpha_1 X^{d-1} + \ldots + \alpha_{d-1} X + \alpha_d. \end{aligned}$$

On peut également retrouver P à partir de P_u, ou trouver un diviseur G de P à partir d'un diviseur Q_u de P_u, en remplaçant X par $a_0 X$ dans P_u ou dans Q_u, puis en rendant primitif le polynôme obtenu.

Signalons que dans la méthode classique de factorisation, le polynôme P est rendu unitaire sur $\mathbb{Z}/(p^m)$ en mettant a_0 en facteur (p étant choisi de façon qu'il ne divise pas a_0). Alors P a ses coefficients majorés par p^m. Cette mise en facteur de a_0 n'est pas possible ici, car le calcul de Φ_n exige que le polynôme de départ soit unitaire sur $\mathbb{Z}[X]$ pour qu'aucun dénominateur n'apparaisse dans le calcul de Φ_n. Évidemment, P_u a des coefficients beaucoup

plus grands que ceux de P. Si on veut comparer les deux méthodes, on devra donc effectuer les calculs du coût en fonction des coefficients de P et non pas en fonction de ceux de P_u. Ces calculs de coût seront effectués plus loin.

Le monomorphisme Φ_n sera défini ci-dessous pour un polynôme P unitaire. On suppose donc dans la suite du paragraphe que P est unitaire.

Notons P' la dérivée de P et considérons la division euclidienne définie par

$$X^{n+1} P' = P . P^* + R \qquad \text{où} \quad \deg R < \deg P. \tag{1}$$

On écrit P^* sous la forme

$$P^* = a_0^* X^n + a_1^* X^{n-1} + \ldots + a_n^*,$$

et on note $\Phi_n(P)$ le polynôme réciproque de P^* :

$$\Phi_n(P) = a_0^* + a_1^* X + \ldots + a_n^* X^n.$$

Le polynôme $\Phi_n(P)$ sera appelé développement logarithmique de P, à l'ordre n, car il est obtenu à partir de la dérivée logarithmique de P.

On démontre facilement que Φ_n vérifie la relation :

$$\Phi_n(P . Q) = \Phi_n(P) + \Phi_n(Q). \tag{2}$$

En effet, d'après la définition de $\Phi_n(P)$ et de $\Phi_n(Q)$, on obtient :

$$X^{n+1} P' = P . P^* + R \qquad \text{où} \quad \deg R < \deg P$$

et

$$X^{n+1} Q' = Q . Q^* + S \qquad \text{où} \quad \deg S < \deg Q.$$

Par suite :

$$X^{n+1} (P . Q)' = X^{n+1} (P' . Q + P . Q') = (P . Q) . (P^* + Q^*) + R . Q + S . P,$$

où $\deg (R . Q + S . P) < \deg P . Q$. Donc (2) est satisfait.

De (1) on déduit les relations suivantes :
pour $j = 0$:

$$a_0^* = d \tag{3}$$

pour $1 \leqq j \leqq d$:

$$a_j^* + a_{j-1}^* a_1 + \ldots + a_1^* a_{j-1} + j a_j = 0, \tag{4}$$

pour $d \leqq j \leqq n$:

$$a_j^* + a_{j-1}^* a_1 + \ldots + a_{j-d}^* a_d = 0. \tag{5}$$

Notons $z_1, \ldots, z_d$ les racines de P (distinctes ou non). Alors

$$P = (X - z_1) \ldots (X - z_d);$$

par suite

$$P^* = (X - z_1)^* + \ldots + (X - z_d)^*.$$

On déduit des relations (3), (4) et (5), que :

$$\Phi_n(X - z_k) = 1 + z_k X + \ldots + (z_k)^j X^j + \ldots$$

Par suite les coefficients a_j^* de P sont égaux à :

$$s_j = \sum_{1 \leqq k \leqq d} (z_k)^j.$$

Les formules (4) et (5) définissent a_j^* comme une fonction linéaire de $a_{j-1}^*, a_{j-2}^*, \ldots$ On peut en déduire a_j^* en fonction de $a_0, a_1, \ldots, a_j$ et les relations ainsi obtenues ne sont rien d'autre que les formules de Newton.

La formule (4) définit aussi $j.a_j$ comme une fonction linéaire de $a_1^*, a_2^*, \ldots, a_j^*$ pour $j \geqq 1$. Par suite les n premiers coefficients de P, à savoir $a_1, \ldots, a_n$ sont définis par les n premiers coefficients de P^*. Donc si $n = d$, la connaissance de $\Phi_n(P)$ suffit à définir P de façon unique.

Si on note $\mathscr{P}^d$ l'ensemble des polynômes unitaires dont le degré est majoré par d, alors Φ_n est un monomorphisme de $\mathscr{P}^d$ dans lui-même, pour $n \geqq d$. Évidemment, Φ_n n'est pas surjectif, car la relation (4) définit $j.a_j$ comme un entier qui n'a aucune raison d'être divisible par j.

Étudions le coût du calcul du développement logarithmique jusqu'à l'ordre n d'un polynôme de degré d. Dans les relations (4) et (5) le nombre total de multiplications de coefficients est égal à

$$S = 1 + 2 + \ldots + d + d + \ldots + d$$

où le nombre de termes de S est égal à n. Les calculs relatifs à (4) et à (5) sont donc majorés par $d.n$ multiplications de coefficients, c'est-à-dire que le coût est donné par

$$d.n.\mathrm{Log}^2 p^m$$

si les calculs sont effectués modulo p^m.

II. UTILISATION DE Φ_n POUR CALCULER UNE EXPRESSION ALGÉBRIQUE RATIONNELLE

Si le polynôme B divise le polynôme A, alors (2) implique aussi que

$$\Phi_n(A/B) = \Phi_n(A) - \Phi_n(B). \tag{6}$$

Pour obtenir $Q = A/B$ à partir de A et de B il suffit donc de connaître le développement logarithmique de Q jusqu'à l'ordre $n = \deg Q = \deg A - \deg B$. On se propose de généraliser la relation (6) à tout couple de polynômes (A, B) en désignant par $[A/B]$ le quotient de la division euclidienne de A par B; montrons donc que :

$$\Phi_n([A/B]) = \Phi_n(A) - \Phi_n(B). \tag{7}$$

Pour cela, appliquons la relation (1) aux polynômes A, B et $Q = [A/B]$; on obtient

$$X^{n+1}A' = A.A^* + R_1 \qquad \text{avec} \quad \deg R_1 < \deg A,$$
$$X^{n+1}B' = B.B^* + R_2 \qquad \text{avec} \quad \deg R_2 < \deg B$$

et

$$X^{n+1}Q' = Q.Q^* + R \qquad \text{avec} \quad \deg R < \deg Q.$$

On a d'autre part $A = B.Q + S$ où $\deg S < \deg B$. Calculons $X^{n+1}A' = X^{n+1}(B'.Q + B.Q' + S')$ en remplaçant $X^{n+1}Q'$ et $X^{n+1}B'$ à l'aide des relations ci-dessus :

$$\begin{aligned} X^{n+1}A' &= Q.(B.B^* + R_2) + B.(Q.Q^* + R) + X^{n+1}S' \\ &= Q.B.(B^* + Q^*) + Q.R_2 + R.B + X^{n+1}S' \\ &= (Q.B + S)(B^* + Q^*) \\ &\quad + Q.R_2 + R.B + X^{n+1}S' - S(B^* + Q^*). \end{aligned}$$

Comme les développements logarithmiques sont faits à l'ordre $n = \deg Q$, on a $\deg B^* = \deg Q^* = n$ et de plus $\deg S' = \deg S - 1 < \deg B - 1$. Par suite

$$\deg(Q.R_2 + R.B + X^{n+1}S' - S(B^* + Q^*)) < \deg B + \deg Q.$$

Il en résulte que B^*+Q^* est le quotient de la division enclidienne de $X^{n+1}A'$ par $A=Q.B+S$. La relation (7) est donc bien vérifiée.

Exemple. – Calcul de la partie entière de la fraction rationnelle

$$F=\frac{(X-7)^{10}(X+3)^7}{(X-2)^{13}}.$$

Pour obtenir la partie entière de F, on a besoin de son développement logarithmique à l'ordre $n=17-13=4$. On calcule donc successivement

$$\Phi_4(X-7)=X^4+7X^3+49X^2+343X+2401$$
$$\Phi_4(X+3)=X^4-3X^2+9X^2-27X+81$$
$$\Phi_4(X-2)=X^4+2X^3+4X^2+8X+16.$$

On en déduit

$$10\Phi_4(X-7)+7\Phi_4(X+3)-13\Phi_4(X-2)$$
$$=4X^4+23X^3+501X^2+3137X+24369$$
$$=4X^4+b_1^*X^3+b_2^*X^2+b_3^*X+b_4^*.$$

On utilise la formule (4) pour calculer les coefficients b_1, b_2, b_3 et b_4 de F. On obtient :

$$b_1=-b_1^*=-23$$
$$2b_2=-b_2^*-b_1.b_1^*=-501+(23)^2=28$$
$$3b_3=-b_3^*-b_1.b_2^*-b_2.b_1^*=-3137+501.23-23.14=8064$$
$$4b_4=-b_4^*-b_1.b_3^*-b_2.b_2^*-b_3.b_1^*$$
$$=-24369+23.3137-14.501-23.2688=-21056.$$

On en déduit que la partie entière de F est égale à

$$X^4-23X^3+14X^2+2688X-5264.$$

III. – FACTORISATION DES POLYNÔMES

Considérons la factorisation de P sur $\mathbb{Z}/(p^m)[X]$ en facteurs irréductibles, $P=a_0.Q_1\ldots Q_r$ et supposons que P ne soit pas irréductible sur $\mathbb{Z}[X]$ et

s'écrive $P = Q \,.\, R$, où

$$Q = b_0 Q_1 \cdot Q_2 \cdots Q_h \qquad \text{et} \qquad R = c_0 Q_{h+1} \cdots Q_r.$$

Considérons les développements logarithmiques des polynômes $Q_1, \ldots, Q_r$ à l'aide du monomorphisme Φ_n avec $n = d$. Le développement de Q est donc égal à $F = \Phi_n(Q_1) + \ldots + \Phi_n(Q_n)$ et celui de R est égal à $G = \Phi_n(Q_{h+1}) + \ldots + \Phi_n(Q_r)$.

Factoriser P sur $\mathbb{Z}[X]$ revient donc à définir deux sommes F et G extraites de $\Phi_n(Q_1) + \ldots + \Phi_n(Q_r)$. Mais F et G doivent être des développements logarithmiques de polynômes Q et R de $\mathbb{Z}[X]$. Le théorème ci-dessous donne des conditions pour que de telles sommes F et G correspondent à des polynômes de $\mathbb{Z}[X]$.

THÉORÈME : *Soit* $\mathrm{P} = a_0 X^d + \ldots a_d$ *un polynôme primitif de* $\mathbb{Z}[X]$, *tel que* $\| P/a_0 \| \geqq 5{,}3$ *et soit* $P_u = X^d + \alpha_1 X^{d-1} + \ldots + \alpha_d$ *le polynôme unitaire associé.*

Soient deux polynômes

$$\mathrm{Q} = X^q + b_1 X^{q-1} + \ldots + b_q \qquad et \qquad R = X^r + c_1 X^{r-1} + \ldots + c_r$$

de degrés q *et* r *tels que* $P_u = Q \,.\, R$ *sur* $\mathbb{Z}/(p^m)[X]$ *avec* $p^m > (4 \| P \|)^d$.

On suppose que les coefficients de Q *et* R *sont calculés dans l'intervalle* $]-1/2p^m,\ 1/2p^m]$ *et on note* b_j^* *et* c_j^* *les coefficients des développements logarithmiques de* Q *et de* R.

Alors les deux assertions suivantes sont équivalentes :

(1) $$P_u = Q \,.\, R \quad sur \ \mathbb{Z}[X];$$

(2) $$\begin{cases} |b_j^*| \leqq n(|a_0| + H(P))^j + (q-n)|a_0|^j \ et \\ |c_j^*| \leqq n(|a_0| + H(P))^j + (r-n)|a_0|^j \quad pour \ 1 \leqq j \leqq d, \end{cases}$$

où

$$n = E\left(\frac{\mathrm{Log} \| P/a_0 \|}{\mathrm{Log}\,(1 + H(P/a_0))} - 1\right),$$

E étant la fonction partie entière.

Remarque : L'hypothèse $\| P/a_0 \| \geqq 5{,}3$ ne sert qu'à simplifier la borne de p^m. Si on la supprime on obtient pour p^m la borne suivante : $(5{,}65 \| P \|)^d$.

La démonstration du théorème utilise les deux lemmes suivants :

LEMME 1 : *Soit* (u_j) *la suite définie par*

$$u_0 = 1$$

et

$$ju_j = A^j(N+S^j).u_0 + A^{j-1}(N+S^{j-1}).u_1 + \ldots + A(N+S).u_{j-1}, \quad \textit{pour } j \geqq 1,$$

les nombres N, A *et* S *étant des entiers positifs.*

Alors :

(i) $u_j = A^j\left(S^j + \binom{N}{1}.S^{j-1} + \ldots + \binom{N+j-1}{j}\right)$;

(ii) $u_j \leqq (1+1/S)^{N-1} A^j (1+S)^j$.

Démonstration : Considérons le polynôme unitaire $A = \sum_{0 \leqq k \leqq j} v_k X^k$ dont le développement logarithmique est égal à $\Phi_n(A) = \sum_{0 \leqq k \leqq n} -NA^k X^k$. La formule (4) permet de calculer les coefficients v_k. On obtient ainsi $v_0 = 1$ et $k.v_k = N.(v_0 A^k + v_1 A^{k-1} + \ldots + v_{k-1} A)$. Par suite

$$k.v_k = (k-1).v_{k-1} A + N.v_{k-1} A = (N+k-1) v_{k-1} A.$$

Donc :

$$v_k = \frac{(N+k-1)(N+k-2)\ldots N}{k.(k-1)\ldots 2.1} A^k = \binom{N+k-1}{k} A^k.$$

Considérons maintenant, le polynôme $B = \sum_{0 \leqq k \leqq j} w_k X^k$ de développement logarithmique égal à $\sum_{0 \leqq k \leqq n} -S^k A^k X^k$. La formule (4) permet de calculer facilement les coefficients w_k; on trouve $w_k = S^k A^k$.

La formule du lemme définissant u_j par récurrence s'écrit sous la forme

$$ju_j = -u_j^* - u_{j-1}^* u_1 - \ldots - u_1^* u_{j-1},$$

avec

$$u_j^* = N.A^j + S^j A^j = v_j^* + w_j^*.$$

Donc d'après la formule (2), les termes u_j sont les coefficients du polynôme $A.B$; ils s'écrivent donc $u_j = \sum_{0 \leqq k \leqq j} v_k w_{j-k}$. Par suite :

$$u_j = \left[S^j + \binom{N}{1} . S^{j-1} + \ldots + \binom{N+j-1}{j} \right] A^j,$$

et (i) est bien vérifié.

Il reste à majorer u_j. Pour cela remplaçons dans le second membre de (i), $\binom{N+k-1}{k}$ par $\binom{N+j-1}{k}$ pour $0 \leqq k \leqq j$. Puis multiplions les deux membres par S^{N-1}. On obtient

$$S^{N-1} u_j \leqq (1+S)^{N+j-1} A^j,$$

donc le lemme est bien vérifié.

LEMME 2 : *Le plus petit commun multiple des nombres* 2, 3, ..., *n noté* $\pi(n)$ *est majoré par* $(2{,}826)^n$.

Démonstration : Si on note $Y(n)$ le logarithme népérien de $\pi(n)$, alors d'après [6] on a $Y(n) \leqq 1{,}038\,83 . n$. Donc, $\pi(n) \leqq (e^{1{,}038\,83})^n = (2{,}826)^n$.

Démonstration du théorème

$1° \Rightarrow 2°$

Q étant un diviseur de P_u, notons Q^0 le diviseur de P associé à Q et b_j^0 les coefficients du développement logarithmique de Q^0. Notons $z_1, \ldots, z_d$ les racines de P, distinctes ou non et $z_1, \ldots, z_q$ celles de Q^0. Le changement de variable substituant X à X/a_0 et rendant P unitaire transforme les racines z_j de P en $a_0 z_j$. On aura donc $|b_j^*| = |a_0|^j . |b_j^0|$.

Considérons la somme $f(z_1, \ldots, z_q) = |z_1|^j + \ldots + |z_q|^j$, et notons $|z_u . z_v \ldots z_w|$ le produit des racines de Q^0 de module minoré par 1. Le produit $|b_0 . z_u . z_v \ldots z_w|$ noté $M(Q^0)$ est appelé la mesure de Q^0 et on a évidemment $M(Q^0) \leqq M(P)$.

Rappelons le résultat suivant démontré par Mignotte dans [5] :

$$M(P) \leqq \| P \|.$$

La somme $f(z_1, \ldots, z_q)$ ci-dessus est majorée par la somme

$$|z_u|^j + |z_v|^j + \ldots + |z_w|^j + 1 + \ldots + 1$$

dans laquelle on a remplacé par 1, les racines $|z_j|$ majorées par 1. Comme le produit $|a_0|.|z_u|.|z_v|...|z_w|$ est majoré par $M(P)$, f sera maximal lorsque ce produit sera égal à $M(P)$. Or chaque racine a une valeur maximale donnée par l'inégalité de Cauchy : $|z_k|<1+H(P/a_0)$, $H(P)$ étant la hauteur de P (maximum de la valeur absolue des coefficients). Les sommes $f(z_1, \ldots, z_q)$ sont donc majorées par

$$B=f(1+H(P/a_0), \ldots, 1+H(P/a_0), 1, \ldots, 1)$$

où on a remplacé le plus grand nombre possible de racines $z_1, \ldots, z_q$ par leur valeur maximale $1+H(P/a_0)$; notons n le plus grand entier tel que $(1+H(P/a_0))^n<\| P/a_0 \|$; alors

$$n=E\left(\frac{\operatorname{Log}\| P/a_0 \|}{\operatorname{Log}(1+H(P/a_0))}-1\right),$$

E étant la fonction partie entière.

On a de plus

$$1+H(P/a_0)<\| P/a_0 \|^{1/n}. \tag{9}$$

On obtient ainsi :

$$|b_j^0| \leqq n(1+H(P/a_0)^j+q-n.$$

Par suite :

$$|b_j^*| \leqq n(|a_0|+H(P))^j+(q-n)|a_0|^j$$

et

$$|c_j^*| \leqq n(|a_0|+H(P))^j+(r-n)|a_0|^j.$$

L'assertion 2° du théorème est donc satisfaite.

Remarque : On pourrait donner un meilleur majorant pour $|b_j^*|$ et $|c^*|$ en remplaçant n par

$$n_1=E\left(\frac{\operatorname{Log}(M(Q^0)/a_0)}{\operatorname{Log}(1+H(P/a_0))}-1\right)$$

dans l'expression majorant $|b_j^*|$ et par $n_2=E\left(\frac{\operatorname{Log}(M(R^0)/a_0)}{\operatorname{Log}(1+H(P/a_0))}-1\right)$ dans l'expression majorant $|c_j^*|$. En remarquant que $M(Q^0)M(R^0)=M(P)$, on

obtient $n = n_1 + n_2$; donc l'un des nombres n_1 ou n_2 est majoré par $1/2\,n$. Mais cette majoration est moins facile à utiliser.

$$2° \Rightarrow 1°.$$

D'après 2°,

$$|b_j^*| \leqq (n(1+H(P/a_0))^j + q - n)\,|a_0|^j;$$

donc d'après (9),

$$|b_j^*| \leqq (n\,\|P/a_0\|^{j/n} + q - n)\,|a_0|^j.$$

Or

$$n \leqq \mathrm{Log}\,\|P/a_0\| \qquad \text{et} \qquad n\,\|P/a_0\|^{j/n} + q - n$$

est une fonction décroissante de n pour ces valeurs de n. On obtient donc

$$|b_j^*| \leqq (\|P/a_0\|^j + q - 1)\,|a_0|^j.$$

Utilisons les relations (3) et (4) pour majorer les coefficients de Q. La relation (3) donne $|b_1| = |b_1^*| \leqq |a_0|(\|P/a_0\| + q - 1)$.

Pour $j > 1$, (4) donne :

$$j|b_j| \leqq |b_1^*|.|b_{j-1}| + \ldots + |b_j^*|.$$

Comme on a $|b_j^*| \leqq |a_0|^j(\|P/a_0\|^j + q - 1)$, on obtient :

$$j|b_j| \leqq |a_0|(\|P/a_0\| + q - 1).|b_{j-1}| + \ldots + |a_0|^j(\|P/a_0\|^j + q - 1).$$

Notons u_j la suite définie par les relations :

$$u_1 = |a_0|(\|P/a_0\| + q - 1)$$

et

$$ju_j = |a_0|(\|P/a_0\| + q - 1)\,u_{j-1} + \ldots + |a_0|^j(\|P/a_0\|^j + q - 1).$$

Il est clair que pour $1 \leqq j \leqq d$, on a $j|b_j| \leqq ju_j$. Or, d'après le lemme 1, on a :

$$u_j \leqq (1 + |a_0|/\|P\|)^{q-2}(|a_0| + \|P\|)^j.$$

Il en résulte donc :

$$j.|b_j| \leqq j.(1 + |a_0|/\|P\|)^{q-2}(|a_0| + \|P\|)^j. \tag{10}$$

On obtient évidemment une majoration analogue avec les coefficients c_j :

$$j.|c_j| \leqq j.(1+|a_0|/\|P\|)^{r-2}(|a_0|+\|P\|)^j. \tag{11}$$

Malheureusement on ne peut pas « simplifier » par j, car on est sur $\mathbb{Z}/(p^m)$ et que $j.b_j$ n'a aucune raison d'être divisible par j sur $\mathbb{Z}$.

Notons N le plus petit commun multiple de 2, 3, ..., q et M le plus petit commun multiple de 2, 3, ..., r. D'après les hypothèses du théorème on a $N.M.P_u = N.Q.M.R$ sur $\mathbb{Z}/(p^m)[X]$.

Le k-ième coefficient de $N.Q.M.R$ noté d_k s'écrit

$$d_k = N.M.(b_k c_0 + b_{k-1} c_1 + \ldots + b_1 c_{k-1} + b_0 c_k),$$

avec $b_j = 0$ (resp $c_j = 0$) pour $j > q$ (resp $j > r$). Majorons d_k en utilisant les majorations (10) et (11); on obtient :

$$d_k \leqq N.M(1+|a_0|/\|P\|)^{q+r-4} \sum_{0 \leqq j \leqq k} s_j.$$

où

$$S_k = \sum_{0 \leqq j \leqq k} s_j$$

avec

$$s_j = (|a_0|+\|P\|)^j (|a_0|+\|P\|)^{k-j}$$

pour

$$j \leqq q \qquad \text{et} \qquad k-j \leqq r$$

et

$$s_j = 0 \qquad \text{pour} \quad j > q \quad \text{et} \quad k-j > r.$$

On vérifie facilement que S_k est une suite croissante, donc sa valeur maximale est atteinte pour $k = d$ et vaut $(|a_0|+\|P\|)^d$. Les coefficients d_k sont donc majorés par

$$N.M.(1+|1+|a_0|/\|P\|)^{d-4}(|a_0|+\|P\|)^d.$$

D'après le lemme 2, on a $N \leqq (2{,}826)^q$ et $M \leqq (2{,}826)^r$. On a donc

$$d_k \leqq (2{,}826)^d (1+|a_0|/\|P\|)^{-4}((|a_0|+\|P\|)/\|P\|)^{2d}\|P\|^d.$$

Si on suppose $\| P/a_0 \|$ supérieur ou égal à 5,3, alors $1+|a_0|/\| P \|$ est majoré par 1,189, donc $(2{,}826)^d((|a_0|+\| P \|)/\| P \|)^{2d} \leqq 4^d$.

D'autre part, la valeur maximale de

$$(1+|a_0|/\| P \|)^{-4}((|a_0|+\| P \|)/\| P \|)^{2d}$$

est obtenue pour $\| P/a_0 \| = 5{,}3$ (en supposant $d \geqq 2$), et dans ce cas $(1+|a_0|/\| P \|)^{-4} < 1/2$. On obtient donc finalement :

$$d_k \leqq 1/2\,(4\| P \|)^d \leqq 1/2\,p^m.$$

Les polynômes $N.M.P_u$ et $N.Q.M.R$ ont donc leurs coefficients compris entre $-1/2\,p^m$ et $1/2\,p^m$. Comme ils sont égaux modulo p^m, ils sont donc égaux sur $\mathbb{Z}[X]$ et le théorème est vérifié.

Remarque : On pourrait améliorer la borne de p^m. Pour cela on ne calcule les développements logarithmiques de Q et R que jusqu'à l'ordre $1/2\,d$, ce qui définit les $1/2\,d$ premiers coefficients de Q et R. Mais on calcule en plus les développements logarithmiques des polynômes réciproques de G et R toujours à l'ordre $1/2\,d$; alors tous les coefficients de Q et R sont définis à partir de ces deux types de développements logarithmiques. Cependant il faut généraliser la définition de Φ_n au cas des polynômes non unitaires ce qui rend plus complexes les relations (4) et (5). Cette généralisation est faite dans [7]; elle donne une borne de p^m de la forme $B^{d/2}$ au lieu de B^d.

IV. ÉTUDE DU COÛT DU NOUVEL ALGORITHME

La première étape de l'algorithme est la factorisation de P sur $\mathbb{Z}/(p)[X]$ par la méthode de Berlekamp. Elle exisge $d^3\,p$ opérations élémentaires, comme le montre Knuth dans [2].

Les calculs de la deuxième étape sont dominés par le calcul de produit de polynômes de degré d, ce qui correspond à d^2 produits de coefficients. Comme les coefficients sont majorés par p^m le coût de la deuxième étape est donné par

$$d^2\ \mathrm{Log}^2\,(p^m).$$

Dans l'algorithme classique on a $p^m \leqq 2^d \| a_0 P \|$, donc le coût est égal à

$$d^2\,(d+\mathrm{Log}\,(\| a_0 P \|))^2.$$

Dans le nouvel algorithme, les coefficients sont bornés par $(4 \| P \|)^d$, donc le coût est égal à

$$d^4 . (2 + \text{Log} \| P \|)^2.$$

Le coût du calcul des images $\Phi_n(Q_1), \ldots, \Phi_n(Q_r)$ a été étudié dans *I*. Ce coût est égal à $d^2 \text{ Log}^2 (p^m)$, soit encore à

$$d^4 . (2 + \text{Log} \| P \|)^2.$$

Le coût total du nouvel algorithme est donc donné par

$$2 d^4 . (2 + \text{Log} \| P \|)^2.$$

Pour la dernière étape de l'algorithme classique, on doit dans le cas où P est irréductible, calculer 2^{r-1} produits de polynômes sur $\mathbb{Z}/(p^m)[X]$, puis 2^{r-1} divisions; le nombre total de multiplications de coefficients est de l'ordre de $2^r d^2$.

Le produit de deux coefficients définis modulo p^m a un coût égal à $\text{Log}^2 p^m = (d + \text{Log} \|_0 P \|)^2$. On obtient donc pour la dernière étape un coût égal à

$$2^r d^2 (d + \text{Log} \| a_0 P \|)^2.$$

Dans le nouvel algorithme, la dernière étape exige le calcul de 2^r sommes de polynômes sur $\mathbb{Z}/(p^m)[X]$; le coût est donc donnée par

$$2^r d^2 . (2 + \text{Log} \| P \|).$$

Pour comparer les deux algorithmes il faut donc comparer le coût de la dernière étape de l'algorithme classique avec le coût de l'étape précédente du nouvel algorithme. Le nouvel algorithme n'est donc intéressant que si

$$2 . d^4 (2 + \text{Log} \| P \|)^2 \leqq 2^r d^2 (d + \text{Log} (\| a_0 P \|))^2,$$

soit

$$d^2 (2 + \text{Log} \| P \|)^2 \leqq 2^{r-1} (d + \text{Log} (\| a_0 P \|))^2,$$

Supposons pour simplifier que $\text{Log} \| a_0 P \|$ soit négligeable par rapport à d. On obtient :

$$2 + \text{Log} \| P \| \leqq 2^{(r-1)/2},$$

soit encore :

$$r > 2 \text{ Log } (2 + \text{Log } \| P \|). \tag{12}$$

Pour étudier cette inégalité, on doit comparer r et d. D'après M. Mignotte et J. L. Nicolas dans [4], le nombre de polynômes P vérifiant

$$| r - \text{Ln } (d) | \geqq \lambda \sqrt{\text{Ln } d} \tag{13}$$

est majoré par $C^{\lambda-2} p^d$ pour tout $\lambda \geqq 0$. D'après M. Mignotte, on peut prendre $C = 4$. Faisons cette hypothèse pour la suite.

Remarquons que le nombre total de polynômes unitaires de $\mathbb{Z}/(p)[X]$, ayant un degré $\leq d$, est égal à p^d. Si on prend donc $\lambda = \sqrt{8}$, on peut affirmer qu'un polynôme sur deux au moins, vérifie la relation

$$| r - \text{Ln } (d) | \leqq \sqrt{8 \text{ Ln } d}.$$

On a donc une fois sur deux :

$$r \geqq \text{Ln } (d) - \sqrt{8 \text{ Ln } d}.$$

En utilisant, la relation (12), on obtient la condition

$$\text{Ln } (d) - \sqrt{8 \text{ Ln } d} - 2 \text{ Log } (2 + \text{Log } \| P \|) > 0. \tag{13}$$

Il est clair que (13) est vérifiée pour d suffisamment grand. Cependant les valeurs de d vérifiant (13) sont de l'ordre du million. On est donc sûr que pour ces valeurs de d, la relation (12) est satisfaite au moins une fois sur deux et qu'alors le nouvel algorithme est le plus performant. Mais la relation (12) peut être satisfaite pour des degrés beaucoup moins élevés et si c'est le cas on a intérêt à utiliser le nouvel algorithme.

V. NOUVEL ALGORITHME DE FACTORISATION

Le nouvel algorithme comporte les étapes suivantes :

1. Factorisation de P sur $\mathbb{Z}/(p)[X]$ où p est un nombre premier choisi de façon que P n'ait pas de facteur carré;

2. Raffinement de la factorisation pour obtenir la factorisation de P sur $\mathbb{Z}/(p^m)[X]$ avec $p^m > 2^d \| a_0 P \|$; soit $Q_1 \ldots Q_r$ cette factorisation; si $r \leqq 2 \text{ Log } (2 + \text{Log } \| P \|)$, alors, on passe à l'étape 3, sinon on passe à l'étape 4;

3. Calcul de tous les sous-produits $Q_u \ldots Q_v$ et divion de P par ces sous-produits, fin de l'algorithme.

4. On vérifie si l'un des facteurs Q_j divise P sur $\mathbb{Z}[X]$; si c'est le cas, fin de l'algorithme, sinon on passe à l'étape 5.

5. Raffinement de la factorisation pour obtenir la factorisation de P sur $\mathbb{Z}/(p^m)[X]$ avec $p^m > (4 \| P \|)^d$;

6. Calcul des $r+1$ développements $\Phi_n(Q_1), \ldots, \Phi_n(Q_r), \Phi_n(P)$ jusqu'à l'ordre d;

7. Calcul des 2^r sommes F extraites de $S = \Phi_n(Q_1) + \ldots + \Phi_n(Q_r)$, puis calcul de $G = \Phi_n(P) - F$.

Si les majorations 2° du théorème sont vérifiées, alors on calcule le produit $Q = Q_u \ldots Q_v$ correspondant à la somme F. D'après le théorème, on est certain que Q est un diviseur de P sur $\mathbb{Z}[X]$.

Le nouvel algorithme n'exige des calculs supplémentaires à ceux de l'algorithme classique que dans le cas où d'une part le nombre de facteurs r modulo p est grand, à savoir supérieur à 2 Log $(2 + \text{Log} \| P \|)$, et où d'autre part aucun facteur modulo p^m n'est un facteur de P sur $\mathbb{Z}[X]$.

Proposons une variante de l'algorithme ci-dessus, consistant à effectuer les calculs modulo $p^m > 2^d \| a_0 P \|$ comme dans la méthode classique, puis à considérer le plus grand entier k_0 tel que

$$n(|a_0| + H(P))^{k_0} + (q-n)|a_0|^{k_0} \leqq p^m.$$

Cette variante comporte les étapes suivantes :

1′. Identique à l'étape 1, ci-dessus;

2′. Identique à l'étape 2, ci-dessus;

3′. Calcul des $r+1$ développements $\Phi_n(Q_1), \ldots, \Phi_n(Q_r), \Phi_n(P)$ jusqu'à l'ordre d modulo $p^m > 2^d \| a_0 P \|$;

4′. Calcul des 2^r sommes F extraites de $S = \Phi_n(Q_1) + \ldots + \Phi_n(Q_r)$, puis calcul de $G = \Phi_n(P) - F$.

5′. Calcul des produits $Q = Q_u \ldots Q_v$ correspondant aux sous-sommes de S qui vérifient les majorations 2° du théorème pour $1 \leqq j \leqq k_0$.

Ainsi les étapes 2′ et 3′ de l'algorithme auront un coût du même ordre de grandeur que dans l'algorithme classique.

Mais à l'étape 5′. On ne calcule que les sous-produits $Q_u \ldots Q_v$ vérifiant les majorations du théorème.

On diminue ainsi la complexité de l'algorithme classique en diminuant le nombre de produits $Q_u \ldots Q_v$ à calculer.

VI. CONCLUSION

La borne prise pour p^m dans le théorème est très souvent excessive. On peut en fait prendre une borne beaucoup plus raisonnable. Par contre la borne donnée pour p^m dans l'algorithme classique est indispensable, quel que soit l'algorithme utilisé. Si on prenait une borne trop petite pour p^m, c'est-à-dire inférieure à $2^q \| a_0 P \|$, alors on pourrait passer à côté d'un facteur, qui aurait un coefficient supérieur à p^m. En effet dans ce cas on aurait $P = Q.R$ modulo p^m avec les coefficients de Q et R réduits modulo p^m, par suite $P = Q.R$ ne serait pas vrai sur $\mathbb{Z}[X]$.

Par contre, dans le nouvel algorithme on peut choisir p^m très inférieur à la borne théorique $(4 \| P \|)^d$, mais supérieur à la borne classique $2^d |a_0| . \| P \|$. Si on désigne, comme dans le paragraphe précédent, par k_0 le plus grand entier tel que $n(|a_0| + H(P))^{k_0} + (q-n)|a_0|^{k_0}$ soit majoré par p^m, alors tout produit $Q = Q_u \ldots Q_c$ qui divise P sur $\mathbb{Z}[X]$, doit vérifier les majorations 2° du théorème pour $1 \leqq j \leqq k_0$.

On obtient ainsi un critère de reconnaissance des diviseurs de P sur $\mathbb{Z}[X]$, avec un coût analogue à celui de l'algorithme usuel.

Rien ne nous permet d'estimer le gain par rapport à l'algorithme classique, mais on peut espérer qu'ainsi le calcul de nombreux produits $Q_u \ldots Q_v$ sera évité, notamment dans le cas d'un polynôme irréductible.

Remarquons d'autre part que si $|a_d| < |a_0|$, où a_d est le terme constant de P, on a intérêt à remplacer P par son polynôme réciproque. La borne classique donnée pour p^m devient alors $2^d \| a_d P \|$.

Signalons aussi une autre approche de l'algorithme classique, visant à diminuer le coût de la dernière étape. Cette variante consiste à factoriser P modulo une dizaine d'entiers premiers p, à l'aide de la méthode de Berlekamp. Ensuite on continue les calculs des étapes suivantes en choisissant celui des entiers p qui a donné le moins de facteurs, soit r. Alors r est très souvent égal au nombre exact de diviseurs de P sur $\mathbb{Z}[X]$ et si c'est le cas la dernière étape disparaît.

Cependant ce procédé multiple par 10 le coût de la première étape, même pour les cas les plus simples. D'autre part pour un degré élevé on a, quel que soit p, r approximativement égal à $\mathrm{Ln}(d)$. Ainsi les différents choix de p donnent des valeurs de r voisines lorsque d est grand, même pour un polynôme irréductible sur $\mathbb{Z}[X]$.

VII. EXEMPLE

On donne le polynôme $P = 3X^6 - 4X^4 - 8X^2 - 1$.

On rend le polynôme unitaire en calculant

$$P_u(X) = 3^5 P(X/3) = X^6 - 12X^4 - 216X^2 - 243.$$

Si on choisit $p = 5$, on doit faire les calculs modulo 5^m, avec, dans l'algorithme classique $5^m > 2^6 . \| a_0 P \| = 1824$; on doit prendre $m \geqq 8$ (pour $m = 4$, $p^m = 625$).

On factorise donc P_u sur $\mathbb{Z}/(5^8)[X]$, en utilisant la méthode classique. On obtient successivement les factorisations sur $\mathbb{Z}/(5)[X]$, ..., $\mathbb{Z}/(5^8)[X]$:

$P_u = (X-1)(X+1)(X-3)(X+3)(X^2-2)$ sur $\mathbb{Z}/(5)[X]$,

puis :

$$P_u = (X+4)(X-4)(X-8)(X+8)(X^2-2) \quad \text{sur } \mathbb{Z}/(5^2)[\mathrm{X}],$$

puis, sur $\mathbb{Z}/(5^4)[X]$:

$$P_u = (X+167)(X-167)(X+79)(X-79)(X^2-257),$$

enfin, sur $\mathbb{Z}/(5^8)[X]$:

$$P_u = (X+155458)(X-155458)(X-155458)(X-59296) \times (X+59296)(X^2+2243).$$

On obtient donc les facteurs suivants :

$Q_1 = X + 155458;$

$Q_2 = X - 155458;$

$Q_2 = X - 59296;$

$Q_4 = X + 59296;$

$Q_5 = X^2 + 2243.$

On calcule les développements logarithmiques des polynômes Q_j jusqu'à l'ordre $\deg P - 1 = 5$. Les coefficients de $\Phi_n(Q_j)$ sont évalués grâce aux formules (3), (4) et (5); on obtient :

$a_0^* = \deg Q_j;$

$a_1^* = -a_1;$

$a_2^* = (a_1)^2 - 2a_0 a_2;$

$a_3^* = -(a_1)^3 + 3a_0 a_1 a_2;$

$a_4^* = (a_1)^4 - 4a_0 (a_1)^2 a_2 + 2(a_0)^2 (a_2)^2;$

Par suite :

$$\Phi_5(Q_1) = 1 - 155\,458\,X + 2\,264\,X^2 - 3\,787\,X^3 + 47\,571\,X^4;$$
$$\Phi_5(Q_2) = 1 + 155\,458\,X + 2\,264\,X^2 + 3\,787\,X^3 + 47\,571\,X^4;$$
$$\Phi_5(Q_3) = 1 + 59\,296\,X - 9\,X^2 - 143\,039\,X^3 + 81\,X^4;$$
$$\Phi_5(Q_4) = 1 - 59\,296\,X - 9\,X^2 + 143\,039\,X^3 + 81\,X^4;$$
$$\Phi_5(Q_5) = 2 - 4\,486\,X^2 - 94\,152\,X^4.$$

On calcule toutes les sous-sommes $F_1 = \Phi_5(Q_j) + \Phi_5(Q_k)$ et $F_2 = \Phi_5(Q_u) + \Phi_5(Q_v) + \Phi_5(Q_w)$ sous la forme

$$A_0^* + A_1^* X + A_2^* X^2 + A_3^* X^3 + A_4^* X^4$$

et

$$B_0^* + B_1^* X + B_2^* X^2 + B_3^* X^3 + B_4^* X^4,$$

puis on examine les majorations 2° du théorème :

$$|A_j^*| \leqq n(|a_0| + H(P))^j + (q-n)|a_0|^j$$
$$|B_j^*| \leqq n|(|a_0| + H(P))^j + (r-n)|a_0|^j,$$

avec ici q et r majorés par 4, $|a_0| = 3$, $|a_0| + H(P) = 11$ et $n = 1$. Ici k_0 est le plus grand entier tel que $11^j + (4-1)3^j$ soit majoré par 5^8, donc $k_0 = 5$.

Les seules sous-sommes de $\Phi_5(Q_1) + \ldots + \Phi_5(Q_5)$ qui vérifient les majorations 2° du théorème sont

$$F_1 = \Phi_5(Q_3) + \Phi_5(Q_4) = 2\,X^2 - 18\,X^2 + 162$$

et

$$F_2 = \Phi_5(Q_1) + \Phi_5(Q_2) + \Phi_5(Q_5) = 4\,X^4 + 42\,X^2 + 990.$$

On ne calcule donc que les produits

$$Q_1\,Q_2\,Q_5 = (X - 155\,458)(X + 155\,458)(X^2 + 2\,243) = X^4 - 21\,X^2 - 27;$$
$$Q_3\,Q_4 = (X + 59\,296)(X - 59\,296) = X^2 + 9.$$

On vérifie que

$$P_u = (X^2 + 9)(X^4 - 21\,X^2 - 27).$$

En remplaçant X par $3X$, puis en rendant primitifs les polynômes obtenus, on obtient la factorisation de P :

$$P=(X^2+1)(3X^4-7X^2-1).$$

REMERCIEMENTS

Je tiens à remercier Maurice Mignotte pour les remarques intéressantes qu'il m'a communiquées.

BIBLIOGRAPHIE

[1] E. R. Berlekamp, *Algebraic Coding Theory*, Mac Graw-Hill, New York, 1968.

[2] D. E. Knuth, *The Art of Computer Programming*, vol. II, Addison-Wesley, 1969.

[3] A. K. Lenstra, H. W. Lenstra et L. Lovasz, *Factoring Polynomials with Rational Coefficients*, Math. Ann., vol. 261, 1982, p. 515-534.

[4] M. Mignotte et J.-L. Nicolas, *Ann. Inst. Henri-Poincaré*, vol. 19, n° 2, p.113-121.

[5] M. Mignotte, *An Inequality About factors of Polunomials*, Math. Comp., vol. 28, 1974, p. 1153-1157.

[6] J. B. Rosser et L. Schoenfeld, *Approximate Formulas for Some Functions of Prime Numbers*, Illinois J. Math., vol. 6, 1962, p. 64-94, Theorem 12.

[7] G. Viry, *Multiplication of Polynomials. Application to the factorization over* $\mathbb{Z}[X]$, EUROCAL 87, Leipzig.

[8] P. S. Wang et L. P. Rothschield, *Factoring Multivariate Polynomials over the Integers*, Math. of Comp., vol. 29, 1975, p. 935-950.