Theoretical Computer Science 1 (1976) 227-235. © North-Holland Publishing Company

ALGORITHMES RELATIFS A LA DECOMPOSITION DES POLYNOMES

Maurice MIGNOTTE

Université Louis Pasteur, Strasbourg, France

Communiqué par A. Schönhage
Reçu le 15 octobre 1974

Résumé. Améliorations et remarques sur un algorithme dû à H. Zassenhaus, qui fournit la factorisation d'un polynôme à coefficients entiers. Puis un algorithme très rapide et très simple qui donne des informations utiles sur la décomposition d'un polynôme modulo p. Applications: tests modulo p d'irréductibilité, de décomposition en facteurs linéaires d'un polynôme, de décomposition d'un idéal en $O(\log p)$ opérations.

Introduction

Nous étudions d'abord le problème de la factorisation d'un polynôme A à coefficients dans Z. L'algorithme que nous considérons est dû à H. Zassenhaus, son principe consiste à utiliser la factorisation de A modulo p^u, u nombre entier, p nombre premier, p^u assez grand (voir [11]).

Soit:

$$A(X) = a_0 X^m + a_1 X^{m-1} + \ldots + a_m.$$

Un changement de variable évident permet toujours, quitte en plus à diviser A par un entier convenable, de supposer A unitaire; soit $a_0 = 1$. On a d'abord besoin, pour un diviseur éventuel de A

$$B(X) = X^n + b_1 X^{n-1} + \ldots + b_n; \qquad b_j \in Z,$$

d'une majoration des $|b_j|$; disons $|b_j| \leqslant M$.

Pour factoriser A dans Z, on le décompose modulo p, p entier premier choisi à l'avance, soit

$$A(X) \equiv A_1(X) \ldots A_r(X) \pmod{p} \tag{1}$$

avec A_k unitaires, puissances de polynômes irréductibles modulo p, deux à deux distincts (soit $A_k = P_k^{e_k}$).

Une construction, essentiellement équivalente au lemme de Hensel, permet ensuite de raffiner cette décomposition en:

$$A(X) \equiv A_1^*(X) \ldots A_r^*(X) \pmod{p^u}, \text{ avec } p^u > 2M$$

(un programme détaillé figure en [12]). A partir de là, Zimmer [11] propose de considérer les différents produits $A^*_{i_1} \dots A^*_{i_j}$ tels que

$$2\sum_{k=1}^{j} \deg(A^*_{i_k}) \leqslant m = \deg A$$

considérés comme polynômes sur $\mathbf{Z}$, les coefficients étant choisis dans l'intervalle $]-p^{u/2}, +p^{u/2}]$, et de tester si l'un d'eux divise A. Si on trouve ainsi un diviseur de A: B_1, on a $A = B_1 B_2$ et on applique à nouveau le procédé tout entier à chacun des B_i, et ainsi de suite. Dans le cas contraire A est irréductible.

Il nous paraît préférable de tester les $A^*_{i_1} \dots A^*_{i_j}$, "remontés" sur $\mathbf{Z}$ comme plus haut, dans l'ordre croissant de leur degré. Ceci permet, en une seule fois, de factoriser A en un produit de polynômes B_j dont chacun est une puissance d'un polynôme irréductible. Il est ensuite facile de trouver C_j, irréductible sur $\mathbf{Z}$, tel que $B_j = C_j^{d_j}$. La connaissance des e_k permet de limiter les valeurs possibles des d_j.

On peut aussi se ramener de manière simple, et rapide, au cas où A est sans facteurs carrés. Il suffit pour cela de calculer $D(X) = \text{p.g.c.d.}(A(X), A'(X))$. Si $D = 1$, A est sans facteur carré, sinon $\deg D \geqslant 1$ et on considère les polynômes D et A/D, et ainsi de suite. Lorsque A est sans facteur carré la méthode proposée ci-dessus fournit directement une décomposition de A en facteurs irréductibles.

Ceci nous amène à chercher une estimation fine de M, puis à étudier le problème de la factorisation d'un polynôme modulo p. D'autres applications sont données à la fin.

1. Majoration des coefficients d'un diviseur d'un polynôme

Le résultat est le suivant:

Théorème 1. *Soient A et B comme plus haut, B divisant A. On a alors la majoration*

$$|b_j| \leqslant \binom{n}{j} \left(\sum_{i=0}^{m} |a_i|^2\right)^{\frac{1}{2}}.$$

Démonstration. Soient $z_1, \dots, z_m$ les racines de A. On a la majoration évidente

$$|b_j| \leqslant \binom{n}{j} \prod_{i=1}^{m} \max(1, |z_i|)$$

(utiliser l'expression des b_j en fonction des racines de B et le fait que les racines de B sont prises parmi les z_i).

Il suffit d'appliquer le Lemme 1 ci-dessous.

Lemme 1. *Soit A unitaire comme ci dessus et soient $z_1, \dots, z_m$ les racines de A dans $\mathbf{C}$ (répétée chacune autant de fois que son ordre de multiplicité). On a la majoration*

$$\prod_{i=1}^{m} \max(1, |z_i|) \leqslant \left(\sum_{i=0}^{m} |a_i|^2\right)^{\frac{1}{2}}. \tag{2}$$

Cette inégalité améliore des résultats successifs de C. L. Siegel, A. O. Gel'fond, N. I. Fel'dman, K. Mahler. Le meilleur d'entre eux, celui de Mahler [3], est obtenu en remplaçant le membre de droite de (2) par $\sum_{i=0}^{m} |a_i|$, sa démonstration utilise la formule de Jensen.

Pour $p \geqslant 1$, et $a_0, \ldots, a_m$ fixés, la fonction $p \mapsto (\sum |a_i|^p)^{1/p}$ est décroissante. L'inégalité (2) est la meilleure possible en ce sens qu'elle n'est plus vraie en général pour $p > 2$ (considérer le polynôme $x^2 - ax - 1$, où a est un nombre positif assez grand).

Le Lemme 1 est vrai pour A à coefficients complexes. Nous avons donné du lemme 1 deux démonstrations différentes, l'une analytique qui repose sur la formule de Parseval [4], l'autre purement élémentaire [5].

Par souci de complétude, nous reproduisons ici la première.

Démonstration du Lemme 1. Supposons que $z_1, \ldots, z_q$ désignent les racines de f appartenant au disque $|z| < 1$. Le polynôme

$$G(z) = A(z) \prod_{j=1}^{q} \frac{1 - \bar{z}_j z}{z - z_j} = \sum_{i=0}^{m} g_i z^i$$

vérifie $|G(z)| = |A(z)|$ pour $|z| = 1$. La formule de Parseval donne

$$\sum_{i=0}^{m} |a_i|^2 = \frac{1}{2\pi} \int_0^{2\pi} |A(e^{i\theta})|^2 d\theta = \frac{1}{2\pi} \int_0^{2\pi} |G(e^{i\theta})|^2 d\vartheta = \sum_{i=0}^{m} |g_i|^2 \geqslant |g_0|^2.$$

La conclusion résulte alors des relations

$$g_0 = G(0) = a_m \prod_{j=1}^{q} (-1/z_j)$$

et

$$\left| \prod_{i=1}^{m} z_i \right| = |a_m|.$$

On peut donc choisir

$$M = \binom{n}{[\frac{n}{2}]} \left(\sum_{i=0}^{m} |a_i|^2 \right)^{\frac{1}{2}}, \quad \text{avec } n = [m/2].$$

On peut comparer cette majoration à celles utilisées respectivement par Zimmer [11] et Zassenhaus [10], à savoir $|b_j| \leqslant \binom{n}{j} R^j$,
avec

$$R = \max (|a_i| + 1),$$

ou

$$R = \max_{1 \leqslant i \leqslant m} \left(\frac{|a_i|}{\binom{m}{i}} \right)^{1/i} (\sqrt[m]{2} - 1)^{-1}$$

Prenons un exemple tiré de [11], soit

$$F(X) = X^{15}+30X^{14}+5X^{13}+2X^{12}+5X+2.$$

Les majorations précédentes de K fournissent respectivement $\max b_j \leqslant 2{,}8\cdot 10^{10}$ et $\leqslant 2{,}7\cdot 10^{9}$, tandis que nous obtenons $M = 1083$.

Notons aussi qu'il n'est pas toujours nécessaire de recourir à de longs calculs pour savoir si un polynôme est irréductible. On a clairement

$$|F(z)-30z^{14}| < 30\,|z|^{14} \text{ si } |z| = 1.$$

La théorème de Rouché montre alors que, dans $|z| \leqslant 1$, les fonctions $F(z)$ et $30z^{14}$ ont le même nombre de zéros. Ainsi, F n'a qu'une racine θ de module $\geqslant 1$ et un raisonnement immédiat permet de conclure à l'irréductibilité de F. (θ est un nombre de Pisot.)

2. Sur la factorisation d'un polynôme modulo p

1. On trouvera de nombreux détails dans le livre de Knuth ([2, pp. 381–390]). Nous nous intéresserons surtout au cas où p est grand et m petit (m est le degré du polynôme). L'algorithme de factorisation de Berlekamp nécessite un nombre d'opérations de l'ordre de $O(pm^3)$. Il n'est donc pas très rapide pour p grad. Knuth donne aussi un algorithme dont le nombre d'opérations est en

$$O(m^2(\log p)^3+m^3(\log p)^2)$$

mais qui ne fournit que le produit des facteurs irréductibles de degré d, pour d varian de 1 à m.

2. Nous nous proposons de décrire un algorithme très rapide et très simple qui sans fournir la factorisation, apporte cependant des informations précises sur la décomposition modulo p.

Théorème 2. *Soient q une puissance d'un nombre premier p, A un polynôme unitaire sur le corps fini $\mathbf{F}_q$, K la plus petite extension de $\mathbf{F}_q$ dans laquelle A se décompose en facteurs linéaires. Alors, on peut déterminer le degré f de K sur $\mathbf{F}_q$ en $O(\log q)$ $\mathbf{F}_q$-opérations.*

Une preuve d'un résultat un peu plus faible utilisant la théorie des suites récurrentes linéaires figure en [6]. Celle qui suit est plus directe.

Démonstration. Les calculs sont effectués dans K. Posons

$$\mathcal{A} = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & 0 & 1 \\ -a_m & -a_{m-1} & & & -a_2 & -a_1 \end{pmatrix}.$$

Sans restreindre la généralité, on peut supposer a_m non nul. Soient $z_1, \ldots, z_s$ les racines de A dans K, et r le maximum des multiplicités des z_i. On sait que $\mathscr{A}$ est semblable à une matrice $D+E$, D diagonale, $E^r = 0$, $DE = ED$. Soit n une puissance de p telle que $n \geqslant r$. Du fait que les coefficients $\binom{n}{k}$ sont divisibles par p pour $0 < k < n$, on a pour h entier positif

$$(D+E)^{nh} = ((D+E)^n)^h = (D^n)^h = D^{nh}.$$

De plus, on a la relation

$$D^{q^f-1} = I.$$

On en déduit

$$\mathscr{A}^{n(q^f-1)} = I. \tag{3}$$

Montrons maintenant que (3) ne peut avoir lieu avec $1 \leqslant f' < f$. Si tel était le cas, de

$$\mathscr{A}(z_i^k \ldots z_i^{k+m-1}) = \mathscr{A}^k(1\, z_1 \ldots z_i^{m-1}),$$

appliqué pour $k = n(q^{f'}-1)$, on déduirait que l'ordre de chaque z_i divise $n(q^{f'}-1)$, donc divise aussi $q^{f'}-1$ (puisque cet ordre est premier à p), ce qui implique $k \subset F_{q^{f'}}$, contrairement à la définition de f. Cette contradiction montre que f est le plus petit entier positif tel que (3) ait lieu. Si F est un majorant de f (il est clair que $F = m!$ convient), il suffit de calculer $(\mathscr{A}^n)^{q^s}$ pour $s = 1, \ldots, F$. Ceci nécessite $O(Fm^3 \log q)$ F_q-opérations.

Ayant précisé que nous nous limitions au cas où m est petit et p grand, nous avons volontairement négligé d'indiquer la dépendance du terme impliqué dans le O en fonction de m. Ce problème présente cependant suffisamment d'intérêt pour que nous l'examinions un moment.

3. Il s'agit de majorer f. Notons que si la décomposition de A est donnée par (1) avec

$$\deg(A_i) = m_i,$$

on a

$$f = \text{p.p.c.m.}(m_i).$$

Si $g(m)$ désigne la valeur maximale possible de f pour m fixé, on a

$$g(m) = \max_{\substack{m_1, \ldots, m_s, s \\ m_1 + \ldots + m_s \leqslant m}} (\text{p.p.c.m.}(m_1, \ldots, m_s)).$$

Par exemple,

$$g(3) = 3, \quad g(4) = 4, \quad g(5) = 6, \quad g(6) = 6, \quad g(7) = 12, \quad g(8) = 15, \quad g(9) = 20, \ldots .$$

Il peut être intéressant de noter que $g(m)$ est aussi l'ordre maximal des éléments du groupe symétrique S_m (cette fonction a été étudiée en détail par J. L. Nicolas [7]). On a donc $f \leqslant m!$, et même f divise $m!$.

Soit

$$g(m) = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad p_1 < p_2 < p_3 < \ldots < p_k,$$

la décomposition en facteurs premiers de $g(m)$ et soient $m_1, ..., m_s$ tels que

$$m_1 + ... + m_s \leqslant m \text{ et } g(m) = \text{p.p.c.m.}(m_1, ..., m_s)$$

et

$$m_1 + ... + m_s \text{ minimal.}$$

Si $p(1), p(2), ...$ désigne la suite croissante des nombres premiers, on considère la suite

$$S(k) = \sum_{i \leqslant k} p(i).$$

Montrons que

$$S(k) \leqslant \sum_{i=1}^{k} p_i \leqslant m. \tag{4}$$

L'inégalité de gauche est évidente, puisque $p(i) \leqslant p_i$, pour $i = 1, ..., k$. Pour démontrer celle de droite, remarquons d'abord que les m_i sont des puissances de nombres premiers. En effet, supposons que l'on ait par exemple $m_1 = m_1' m_1''$ avec $(m_1', m_1'') = 1, m_1' > m_1'' \geqslant 2$, on a aussi

$$g(m) = \text{P.P.C.M.}(m_1', m_1'', m_2, ..., m_s)$$

avec

$$m_1' + m_1'' + m_2 + ... + m_s < m_1 + m_2 + ... + m_s,$$

puisque

$$m_1' + m_1'' < 2m_1' \leqslant m_1' m_1'' = m_1,$$

ce qui contredit la minimalité de la somme des m_i. Sachant maintenant que les m_i sont des puissances de nombres premiers, la minimalité de $m_1 + ... + m_s$ montre que les m_i sont supérieurs à 1 et deux à deux premiers entre eux. On a donc $k = s$, et en choisissant convenablement la numérotation, $m_i = p_i^{\alpha_i}$. La seconde inégalité est alors claire:

$$p_1 + ... + p_k \leqslant p_1^{\alpha_1} + ... + p_k^{\alpha_k} = m_1 + ... + m_k \leqslant m.$$

On en déduit la majoration

$$g(m) = p_1^{\alpha_1} ... p_k^{\alpha_k} \leqslant \left(\frac{\sum p_i^{\alpha_i}}{k} \right)^k \leqslant \left(\frac{m}{k} \right)^k \tag{5}$$

d'après le fait bien connu que le maximum d'un produit de nombres positifs, dont la somme est constante, est atteint lorsque ces nombres sont égaux. Remarquons enfin que, d'après le théorème des nombres premiers, on a aussi

$$S(k) \sim \frac{k^2 \log k}{2}. \tag{6}$$

Soit y tel que $y^2 \log y = 2m$, ce qui implique $y \sim 2(m/\log m)^{1/2}$. D'après (4) et (6), on a

$$k \leqslant (1 + o(1))\, y = (2 + o(1))\, (m/\log m)^{1/2} \; (\leqslant m/e \text{ pour } m \text{ assez grand}). \tag{7}$$

Puis de (5) et (7) et de la croissance de la fonction $(m/x)^x$ pour $x \leqslant m/e$ résulte

l'inégalité

$$g(m) \leqslant \exp((1+o(1))\sqrt{m \log m}).$$

Cette majoration est essentiellement la meilleure possible, puisque g vérifie la condition

$$\log g(m) \sim \sqrt{m \log m},$$

résultat dû à Landau, et qui m'a été signalé par M. P. Schützenberger (voir [7]).

Nous avons obtenu le résultat suivant, qui précise le Théorème 2.

Proposition 1. *Le nombre N d'opérations considéré dans le Théorème 2 vérifie*

$$N \leqslant Cm^3 g(m) \log p, \qquad C \text{ constante},$$

avec

$$g(m) = \max_{\substack{m_1,\ldots,m_s,s \\ m_1+\ldots+m_s=m}} (\text{p.p.c.m.}(m_1, \ldots, m_s));$$

et on a

$$g(m) = \exp((1+o(1))\sqrt{m \log m}).$$

Ceci montre en particulier que cet algorithme ne présente un intérêt que pour des valeurs de m assez petites. Comme me l'a fait remarquer J. Berstel, on peut donner une forme effective à la Proposition 1. En 1939, Rosser a démontré l'inégalité remarquable $p(n) > n \log n$ (voir [8] pour des résultats plus précis). On a donc la minoration

$$S(k) \geqslant \sum_{1 \leqslant n \leqslant k} n \log n.$$

Pour estimer le membre de droite, on peut utiliser la formule d'Euler Mac-Laurin (voir, par exemple, [1, p. 303]), soit

$$\sum_{n=1}^{k} f(n) \geqslant \int_1^k f(x)\,dx + \frac{1}{2}(f(1)+f(n)) + \frac{1}{12}(f'(n)-f'(1)) - \frac{1}{\pi}\int_1^n |f^{(3)}(t)|\,dt,$$

ce qui donne ici

$$\sum_{n=1}^{k} n \log n \geqslant \frac{k^2}{2}(\log k - 1/2) + (k \log k)/2 + (\log k)/12 - \frac{1}{\pi k}$$

$$\geqslant \frac{k^2}{2}\left(\log k - \frac{1}{2}\right).$$

Dans notre problème, k vérifie donc

$$k^2(\log k - 1/2) \leqslant 2m,$$

ce qui implique

$$k \leqslant 2\sqrt{m/\log m}\,(1+(\log m)^{-1}) =: K'.$$

Pour $m \geqslant 24$, on a $K' \leqslant m/e$, et donc

$$g(m) \leqslant (m/K')^{K'} \quad \text{pour } m \geqslant 24.$$

3. Applications

1. *Décomposition d'un polynôme en facteurs linéaires sur* $\mathbf{F}_q$.

On a déjà remarqué que le Théorème 2 est vrai sur $\mathbf{F}_q$. Pour savoir si un polynôme se décompose en facteurs linéaires sur $\mathbf{F}_q$, il suffit de tester si $[K: \mathbf{F}_q] = 1$. On obtient alors le résultat suivant.

Théorème 3. *Pour savoir si un polynôme de degré m se décompose en facteurs linéaires dans le corps fini* $\mathbf{F}_q$, *il suffit de* $O(m^3 \log q)$ *opérations.*

2. *Un test d'irréductibilité modulo p.*

Si le polynôme A considéré est de degré *m primaire**, on a $[K: \mathbf{F}_p] = m$ si, et seulement si, A est irréductible modulo p. D'où le théorème suivant.

Théorème 4. *Pour savoir si un polynôme de degré m primaire est irréductible modulo p, il suffit de* $O(m^3 \log p)$ *opérations.*

3. *Décomposition des idéaux dans un corps de nombres.*

Soit L une extension algébrique de degré fini sur Q, $L = Q(\vartheta)$, où ϑ admet A pour polynôme minimal. Soit p un nombre premier qui ne divise pas le discriminant de A, on sait depuis Kummer que la décomposition de A modulo p permet de déterminer la décomposition de l'idéal (p) dans L (voir par exemple [9], th. 4-9-1, et l'exercice 4-9-2 où on montre que ce résultat est vrai dans des conditions plus générales). Par souci de simplicité, limitons nous au cas où L est un corps cubique. On a alors les trois possibilités suivantes

(i) A est irréductible modulo p; alors (p) est irréductible dans L;

(ii) $A \equiv A_1 A_2 \pmod p$, A_i irréductibles; alors $(p) = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_i$ irréductibles;

(iii) $A \equiv A_1 A_2 A_3 \pmod p$ et $(p) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$.

On peut distinguer facilement le cas (ii) des deux autres. Considérons en effet le discriminant D de A. Soient z_1, z_2, z_3 les racines de A dans une extension de $\mathbf{F}_p$ (avec $p \nmid D$). On a

$$D = \delta^2, \quad \text{avec } \delta = (z_1 - z_2)(z_2 - z_3)(z_3 - z_1).$$

Dans le cas (i), les z_i sont dans $\mathbf{F}_p$, donc δ aussi et D est un résidu quadratique modulo p, soit $\left(\frac{D}{p}\right) = +1$ (symbole de Legendre). Dans le cas (ii) on a, avec une numérotation convenable, $z_1 \in \mathbf{F}_p$, z_2 et $z_3 \in \mathbf{F}_{p^2}$ et $\notin \mathbf{F}_p$. Si σ désigne l'isomorphisme qui envoie x sur x^p, on a $\sigma(z_1) = z_1$, $\sigma(z_2) = z_3$, $\sigma(z_3) = z_2$, donc $\sigma(\delta) = -\delta$, ce qui montre que $\delta \notin \mathbf{F}_p$ et donc que $\left(\frac{D}{p}\right) = -1$. Dans le dernier cas, on a $z_i \in \mathbf{F}_p$,

* C'est à dire, puissance d'un nombre premier.

et $\notin \mathbf{F}_p$, $i = 1, 2, 3$ et. avec une numérotation convenable, $\sigma(z_1) = z_2$, $\sigma(z_2) = z_3$, $\sigma(z_3) = z_1$, donc $\sigma(\delta) = \delta$ et $\left(\frac{D}{p}\right) = 1$. On distingue ensuite le cas (i) de (iii) en appliquant le Théorème 3 sur $\mathbf{F}_p$. En résumé:

Théorème 5. *Soit L un corps cubique sur Q, $L = Q(\vartheta)$, où ϑ admet A pour polynôme minimal (A unitaire, à coefficients entiers). Soit p un nombre premier qui ne divise pas le discriminant D de A. Alors on peut déterminer le type de décomposition de l'idéal (p) dans L en $O(\log p)$ opérations. (La décomposition $(p) = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1$ et $\mathfrak{p}_2$ premiers correspont au cas $\left(\frac{D}{p}\right) = -1$.)*

Remarque. Ce résultat peut être particulièrement utile quand on cherche, pour L fixé, le comportement d'un grand nombre d'idéaux (p). Rappelons que l'algorithme proposé consiste seulement à calculer, modulo p, une puissance convenable d'une certaine matrice à coefficients entiers. De plus, d'après la loi de réciprocité quadratique ([9, Th. 7-3-3]), $\left(\frac{D}{p}\right) = -1$ équivaut à ce que p appartienne à une union finie de progressions arithmétiques (qu'il est facile de déterminer).

Bibliographie

[1] J. Dieudonné, Calcul Infinitésimal (Hermann, Paris, 1968).

[2] D. E. Knuth, The Art of Computer Programming, vol. 2, Seminumerical Algorithms (Addison-Wesley, Reading, Mass., 1971).

[3] K. Mahler, An application of Jensen's formula to polynomials, Mathematika 7 (1960) 98–100.

[4] M. Mignotte, Critères d'irréductibilité de polynômes sur un corps de nombres, Enseignement Math. 18 (1972) 191–200.

[5] M. Mignotte, An inequality about factors of polynomials, Math. Comp. (à paraître).

[6] M. Mignotte, Suites récurrentes linéaires, Séminaire Delange-Pisot-Poitou (Groupe d'études de théorie des nombres) (1973/74) no G14, 9p

[7] J. L. Nicolas, (Thèse) Ordre maximal d'un élément du groupe S_n des permutations et "Highly composite numbers", Bull. Soc. Math. France 97 (1969) 129–191.

[8] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 291–311.

[9] E. Weiss, Algebraic Number Theory (McGraw-Hill, New York, 1963).

[10] H. Zassenhaus, On Hensel factorisation I, J. Number Theory 1 (1969) 291–311.

[11] H. G. Zimmer, Computational Problems, Methods, and Results in Algebraic Number Theory, Lecture Notes in Math. 262 (Springer, Berlin, 1972).

[12] H. G. Zimmer, Factorisation of polynomials according to a method of Zassenhaus, University of California, Los Angeles, 1969.