Astérisque

MAURICE MIGNOTTE

Factorisation des polynômes sur un corps fini

Astérisque, tome 38-39 (1976), p. 149-157

<http://www.numdam.org/item?id=AST_1976__38-39__149_0>

Société Mathématique de France
Astérisque 38-39 (1976) p.149-157

FACTORISATION DES POLYNOMES SUR UN CORPS FINI

par Maurice MIGNOTTE

1. Introduction.

La connaissance de la factorisation d'un polynôme sur un corps fini peut intéresser en particulier un théoricien des codes ou un arithméticien. En ce qui concerne ce premier, le lecteur pourra s'en convaincre en consultant l'ouvrage de E.R. BERLEKAMP [1], dont le sixième chapitre est consacré à ce problème. Par ailleurs, chacun sait l'importance de la réduction modulo un nombre premier en arithmétique. Nous allons aborder l'analyse de divers algorithmes liés à cette question.

2. Le coût des opérations dans un corps fini.

Nous nous plaçons dans un corps fini $\mathbb{F}_q$ à q éléments. Si $q = p^m$ avec p premier, nous considérons que les éléments du corps $\mathbb{F}_q$ sont donnés par leurs composantes dans une base $(1, x, \ldots, x^{m-1})$ du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_q$, où x est un élément fixé de $\mathbb{F}_q$ de degré m sur $\mathbb{F}_p$.

1. L'addition.

L'addition de deux éléments de $\mathbb{F}_q$ équivaut à m additions dans $\mathbb{F}_p$. Elle nécessite donc un temps $m.O(\text{Log } p)$, soit $O(\text{Log } q)$.

2. La multiplication.

Supposons connue la décomposition des éléments $x^m, x^{m+1}, \ldots, x^{2m-2}$ sur la base $(1, x, \ldots, x^{m-1})$. Le produit de deux éléments

de $\mathbb{F}_q$ se ramène à m^2 produits dans $\mathbb{F}_p$ suivis d'au plus m^2 additions dans $\mathbb{F}_p$. La méthode usuelle de multiplication de deux entiers positifs majorés par p nécessite $O(\text{Log } p)$ additions. D'où un temps total en $(\text{Log}^2 q)$.

La méthode de Schönhage-Strassen (voir [3], chap. 4, § 3.3) permet d'effectuer la multiplication de deux entiers modulo p en un temps $O(\text{Log } p \text{ Log Log } p \text{ Log Log Log } p)$.

3. La division.

Pour calculer $y z^{-1}$ on multiplie y et z^{-1}. Il suffit donc de considérer le calcul de l'inverse d'un élément. Pour un élément x non nul de $\mathbb{F}_q$, on a tout simplement

$$x^{-1} = x^{q-2} .$$

Le calcul de x^n peut s'effectuer ainsi : si $n = \sum_{j=0}^{i} e_j 2^j$, $e_j \in \{0, 1\}$, est le développement binaire de n, on a

$$x^n = \prod_{0 \le j \le i,\ e_j \neq 0} x^{2^j} . \tag{1}$$

Par cette méthode, le calcul de x^{-1} ne nécessite pas plus de $2(\text{Log } q/\text{Log } 2)$ multiplications. Si $\mathfrak{M}(q)$ et $\mathfrak{D}(q)$ désignent respectivement le coût de la mutiplication et de la division dans le corps $\mathbb{F}_q$, on a

$$\mathfrak{D}(q) = O(\text{Log } q \cdot \mathfrak{M}(q)) .$$

Nous ignorons si cette majoration peut être améliorée dans le cas général.

Cependant, dans le cas particulier du corps $\mathbb{F}_p$, ces résultats ne sont pas les meilleurs possibles. Considérons en effet le calcul de l'inverse modulo p d'un entier x, $0 < x < p$.

L'algorithme d'Euclide permet le calcul d'entiers u et v tels que

$$ux + vp = 1 .$$

Modulo p, $u = x^{-1}$. Cet algorithme prend un temps $O(\text{Log}^2 p)$ (voir [3], exercice 4.5.2.30). L'algorithme de SCHÖNHAGE [6] permet le calcul de x^{-1} au bout d'un temps $O(\text{Log } p(\text{Log Log } p)^2 \text{ Log Log Log } p)$.

En tout cas, par les méthodes considérées ici, la division dans $\mathbb{F}_q$, même pour $q = p$, est plus coûteuse que la multiplication. On cherchera donc à minimiser le nombre de divisions.

3. Détermination de la période d'un polynôme.

1. Soit

$$f(X) = X^d - a_1 X^{d-1} - \ldots - a_d , \quad a_d \neq 0 ,$$

le polynôme, à coefficients dans $\mathbb{F}_q$, dont on étudie la factorisation. La période t du polynôme f est le plus petit entier positif j tel que $f(X)$ divise $X^j - 1$.

Si

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ a_d & a_{d-1} & & \dots & & a_1 \end{pmatrix} ,$$

la relation

$$(2) \qquad \begin{pmatrix} X^k \\ X^{k+1} \\ \\ X^{k+d-1} \end{pmatrix} = A^k \begin{pmatrix} 1 \\ X \\ \\ X^{d-1} \end{pmatrix} \quad \text{modulo } f(X) , \quad k \in \mathbb{N} ,$$

montre que cette période est égale au plus petit entier positif j tel que $A^j = I$ (matrice unité).

2. Soit $K = \mathbb{F}_{q^r}$ l'extension de $\mathbb{F}_q$ engendrée par les racines de f et soit n la plus petite puissance de p au moins égale à la multiplicité de ces racines. On démontre que t est un diviseur de $n(q^r-1)$, un multiple de n, et ne divise pas $n(q^{r'}-1)$ pour $0 < r' < r$. D'où l'intérêt du calcul de r pour la détermination de t.

3. La relation (2) montre que r est le plus petit entier positif j tel que

$$A^{n(q^j-1)} = I .$$

La détermination de r est ramenée au calcul de certaines puissances de A, et le truc utilisé en (1) montre que $O(r \operatorname{Log} q + \operatorname{Log} n)$ multiplications de matrices $d \times d$, à coefficients dans $\mathbb{F}_q$, suffisent. Le

calcul direct de A^k -par la méthode usuelle- nécessite $O(d^3 \text{ Log } k)$ additions et multiplications dans $\mathbb{F}_q$. Comme l'indique KNUTH ([3], p. 388), ici il est plus efficace de calculer $1, X, X^2, \ldots, X^{2^i}$ modulo f. Le calcul de X^k modulo f est possible en $(d^2 \text{ Log } k)$ opérations. Ainsi, la détermination de r est possible en

$$O(d^2(r \text{ Log } q + \text{Log } n)) = O(d^2(r \text{ Log } q + \text{Log } p))$$

additions et multiplications dans $\mathbb{F}_q$.

4. Voici un exemple d'application arithmétique du calcul de r. Si p est un nombre premier alors le type de décomposition de l'idéal (p) dans un corps cubique peut être déterminé en $O(\text{Log } p)$ additions et multiplications modulo p (voir [6]).

5. Examinons maintenant le comportement de r. On démontre (voir par exemple [6]) la majoration

$$r \leq \exp(c \sqrt{d \text{ Log } d}),$$

pour une certaine constancte c, nécessairement au moins égale à 1. La valeur de r croît donc très vite avec d. En [5], R. J. Mac ELIECE conjecture que la valeur moyenne de r croît linéairement avec d. Plusieurs arguments heuristiques conduisent à penser qu'il est plus prudent de conjecturer que cette valeur moyenne est majorée par une fonction du type $\exp(c' \text{ Log}^2 d)$.

4. L'algorithme de Berlekamp.

1. On travaille dans l'algèbre $R = \mathbb{F}_q[X]/(f(X))$ des polynômes sur $\mathbb{F}_q$ réduits modulo f. On considère dans R l'équation (linéaire !)

$$g^q - g = 0 \quad . \tag{3}$$

Si $f = \prod_{i=1}^{k} f_i^{e_i}$, où les f_i sont irréductibles (sur $\mathbb{F}_q$) et distincts, et si $R_i = \mathbb{F}_q[X]/(f_i(X)^{e_i})$ l'isomorphisme naturel $R \simeq R_1 \times \dots \times R_k$ permet de montrer que les solutions de l'équation (3) constituent un espace de dimension k sur $\mathbb{F}_q$.

La factorisation de f est obtenue de la manière suivante. Pour une solution g de l'équation (3), on a

$$f(X) = \prod_{x \in \mathbb{F}_q} (f(X),\ g(X)-x) \tag{4}$$

(où (a, b) désigne le p. g. c. d. des polynômes a et b). En faisant parcourir à g une base des solutions de (3) on aboutit à la décomposition $f = h_1 \dots h_k$, où $h_i = f_i^{e_i}$ pour $i = 1, \dots, k$.

2. Examinons le calcul des solutions de l'équation (3). Soit Q la matrice associée à cette équation linéaire, la i-ème ligne de Q représente $X^{q(i-1)}$ réduit modulo f. Le calcul de Q ne nécessite que $O(d^2 \operatorname{Log} q)$ additions et multiplications dans $\mathbb{F}_q$ (voir [3], p. 388-389). BERLEKAMP propose de calculer une base du noyau de $Q-I$ en triangularisant cette matrice. Un algorithme est décrit en [3], p. 386-389, il nécessite $O(d^3)$ $\mathbb{F}_q$-opérations, dont des divisions.

Mac ELIECE remarque que si m_i désigne le plus petit entier positif tel que $X^i = X^{iq^{m_i}}$ modulo f alors les polynômes

$$T_i(X) = X^i + X^{iq} + \ldots + X^{iq^{m_i-1}}$$

sont solutions de (3). Si f est sans facteur carré, la famille $T_1, T_2, \ldots, T_{t-1}$ engendre l'espace des solutions de (3). Cette remarque présente un intérêt lorsque t n'est pas très grand par rapport à d.

3. Pour q grand, les calculs impliqués par la décomposition (4) deviennent très longs. Il faudrait pouvoir déterminer l'ensemble S des valeurs de x qui fournissent un terme (f(X), g(X)-x) non trivial.

Au lieu de (4), ZASSENHAUS [8] considère l'équation

$$f(X) = \prod_{x \in S} (f(X), g(X)-x) .$$

Si $G(X) = \prod_{x \in S} (X-x) = \sum G_i X^i$, cette équation montre que f divise G(g(X)), donc on détermine G en calculant 1, g, g^2, ... dans R jusqu'à ce qu'on trouve une puissance de g dépendant linéairement des puissances inférieures. Il n'y a plus qu'à déterminer les racines de G ... ce qui, en général, est assez long.

En [2], § 3 et 4, BERLEKAMP présente un algorithme complexe mais efficace qui ramène aussi le problème de la factorisation de f grâce aux relations (4) à la détermination des racines de certains polynômes.

4. Recherche des racines d'un polynôme.

1. Les procédés décrits par BERLEKAMP ([2], § 5 et 6) permettent de se limiter au cas de la recherche des racines d'un polynôme qui se factorise complètement dans le corps $\mathbb{F}_p$.

2. Soit

$$f(X) = \prod_{1}^{d} (X-s_i) ,$$

où les s_i sont des éléments de $\mathbb{F}_p$. Un procédé standard permet de se ramener au cas où les s_i sont distincts, ce qu'on supposera.

3. La décomposition

$$f(X) = (f(X),\ X^{(p-1)/2}-1)(f(X),\ X^{(p-1)/2}+1)$$

sépare les s_i suivant qu'il sont ou non résidus quadratiques modulo p. Si cette décomposition est triviale, on considère au lieu de $f(X)$ un polynôme de la forme $f(X-s)$. La probabilité qu'une valeur de s conduise à une décomposition triviale est voisine de 2^{-d}. En général on aboutit donc à une décomposition non triviale au bout d'un petit nombre de choix de s.

Notons que dans le cas quadratique on sait déterminer les racines en $O(\text{Log } p)$ opérations (voir [4]).

5. Factorisation sur $\mathbb{Z}$.

ZASSENHAUS [8] présente un algorithme qui ramène la factorisation d'un polynôme dans $\mathbb{Z}$ à sa factorisation dans $\mathbb{Z}/M\mathbb{Z}$, pour

un entier M assez grand. Quelques remarques sur cet algorithme figurent en [6] , ainsi qu'un résultat permettant de choisir des valeurs de M nettement plus petites que celles indiquées par ZASSENHAUS.

REFERENCES

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

[2] E. R. BERLEKAMP. - Factoring polynomials over large finite fields, Math. of Computation, v. 24, n°111, 1970, 713-735.

[3] D. E. KNUTH. - The Art of Computer Programming, vol. II ; Semi numerical Algorithms, Addison-Wesley, Reading, Massachussets, 1969.

[4] D. H. LEHMER. - Computer technology applied to the theory of numbers, in Studies in Number Theory, p. 117-151, ed. W. J. Leveque, Englewood Cliffs, Prentice Hall, 1969.

[5] R. J. Mac ELIECE. - Factorization of polynomials over finite fields, Math. of Computation, 23, n° 108, 1969, 861-868.

[6] M. MIGNOTTE. - Algorithmes relatifs à la décomposition des polynômes, Theorical Computer Science,

[7] A. SCHÖNHAGE. - Schnelle Berechnung von Kettenbruchenwicklungen, Acta Informatica 1, 1971, 139-144.

[8] H. ZASSENHAUS. - On Hensel factorization I , J. Number Theory, v. 1, 1969, 291-311.

Maurice MIGNOTTE
Centre de Calcul
7, rue René Descartes
67084 STRASBOURG CEDEX