ELSEVIER

Theoretical Computer Science 244 (2000) 263–265

Theoretical Computer Science

www.elsevier.com/locate/tcs

n and similar papers at core.ac.uk

provid

Note

Applications of the representation of finite fields by matrices

Eric Kern, Maurice Mignotte*

Université Louis Pasteur, Département de Mathématique, 7, Rue René Descartes 67084 Strasbourg, France

Received 29 June 1999; revised 30 December 1999; accepted 28 February 2000

Abstract

We consider the matrix well-known representation of $K[X]/(P)$, when P is monic irreducible polynomial, with coefficients in K. This representation enables us to give a fast algorithm to solve the equation $x^d = a$ in a finite field. © 2000 Elsevier Science B.V. All rights reserved.

Résumé

Nous considérons la représentation matricielle bien connue de $K[X]/(P)$, où P est un polynôme à coefficients dans K, unitaire et irréductible. Cette représentation nous permet de donner un algorithme rapide de résolution de l'équation $x^d = a$ dans un corps fini. © 2000 Elsevier Science B.V. All rights reserved.

1. La représentation matricielle

Soit R un anneau intègre et $P = X^d + a_1X^{d-1} + \cdots + a_d$ un polynôme unitaire à coefficients dans R. On désigne par A la matrice compagnon de P, c'est-à-dire

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_d \\ 1 & 0 & \dots & 0 & -a_{d-1} \\ 0 & 1 & \dots & 0 & -a_{d-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

* Corresponding author. Tel.: 88-41-6418, 88-41-6348; fax: 88-61-9069.
E-mail address: mignotte@math.u-strasbg.fr (M. Mignotte).

0304-3975/00/$ - see front matter © 2000 Elsevier Science B.V. All rights reserved.
PII: S0304-3975(00)00150-X

Soit θ l'image de X dans $R[X]/(P)$. Alors A n'est rien d'autre que la matrice de l'application $x \mapsto \theta x$ dans la base $1, \theta, \ldots, \theta^{d-1}$. Comme $P(\theta) = 0$, on a $P(A) = 0$, sans utiliser le théorème de Cayley–Hamilton. On montre aussi que P est le polynôme minimal de A. L'algèbre $R[X]/(P)$ est isomorphe au sous-anneau $R[A]$ de l'anneau $\mathbb{M}_d(R)$ des matrices $d \times d$ à coefficients dans R. L'anneau R a pour image $R \cdot I$ dans $R[A]$, où I désigne la matrice identité de $\mathbb{M}_d(R)$. Si $R = K$ est un corps et si P est irréductible, alors $K[X]/(P)$ est le corps de rupture du polynôme P.

Dans $R[A]$ les opérations arithmétiques usuelles, addition, multiplication et calcul de l'inverse s'effectuent comme dans l'anneau quotient $R[X]/(P)$, mais avec cependant deux différences: on doit manipuler des matrices ce qui nécessite plus d'opérations, par contre il n'y a pas à faire de réductions modulo P. Une opération pour laquelle notre représentation semble bien adaptée est l'élévation à une puissance, c'est elle que nous utiliserons dans les paragraphes suivants, en particulier pour la résolution de l'équation $x^d = a$ dans un corps fini.

2. Application à la résolution rapide de l'équation $x^d = a$ dans un corps fini

On suppose désormais que K est un corps fini de cardinal $q = p^n$, avec p premier. On considère $a \in K^\times$ tel que a soit une puissance d–ième dans K, où d est un entier divisant $q-1$ (c'est le seul cas non trivial). On a donc $a^{(q-1)/d} = 1$. On suppose que l'on a trouvé un polynôme $P \in K[X]$, unitaire et irréductible, tel que $P(0) = (-1)^d a$. C'est la partie *probabiliste* de notre algorithme. Notons que la "probabilité" qu'un polynôme unitaire de $K[X]$ de degré d soit irréductible est voisine de $1/d$. On considère A, la matrice compagnon de P. Nous affirmons que

$$A^{\frac{q^d-1}{d(q-1)}} = xI,$$

où $x \in K$ vérifie $x^d = a$. Le nombre d'opérations (dans $K[A]$) nécessaires à ce calcul est en $O(d \log q)$.

Posons $B = A^{(q^d-1)/(d(q-1))}$. Comme les solutions $M \in K[A]$ de l'équation $P(M) = 0$ sont $A, A^q, \ldots, A^{q^{d-1}}$, on a $B^d = (-1)^d P(0) I = a \cdot I$. Enfin, du fait que a est une puissance d–ième, les solutions de l'équation $x^d = a$ appartiennent toutes au corps K, donc B vérifie bien $B = x \cdot I$ avec $x^d = a$. Il est utile de noter qu'il n'est pas nécessaire de tester l'irréductibilité de P: on fait les calculs ci-dessus avec un premier choix de P, si on a trouvé $x^d = a$ on s'arrête, sinon on essaie un nouveau P...

Dans le cas particulier où $d = 2$, cette méthode est une variante de la méthode de Lehmer [3] qui consiste à calculer les termes d'une certaine récurrence binaire (de matrice-compagnon A). On peut aussi remarquer que dans ce cas, si $P = X^2 - bX + a$ alors P est irréductible si, et seulement si, $b^2 - 4a$ n'est pas un carré dans K.

Remarque. Dans l'ouvrage de Cohen [2, pp. 32–36], on trouve une étude des algorihmes pour résoudre $x^2 = a$ modulo p, en plus de la méthode générale de recherche

des racines d'une équation polynomiale modulo p, l'auteur présente la méthode de Schoof — la seule non probabiliste connue — et une méthode de Tonelli–Shanks.

3. Application à la détermination de la décomposition des idéaux d'un corps de nombres

Dans le cas où $K = \mathbb{Q}$ avec P irréductible, la représentation matricielle passe automatiquement au quotient modulo un nombre premier p. Notons O l'anneau des entiers du corps de nombres $\mathbb{Q}[\theta]$, avec θ comme plus haut. Lorsque l'indice de $\mathbb{Z}[\theta]$ dans O n'est pas divisible par p, l'injection $\mathbb{Z}[\theta] \to O$ induit un isomorphisme $\mathbb{F}_p[\theta] \sim O/pO$ (cf. [1, pp. 92–93]). Si le polynôme P se décompose modulo p en

$$\bar{P} = P_1^{e_1} \cdots P_r^{e_r}, \qquad e_1, \ldots, e_r \geqslant 1,$$

où les P_i appartiennent à $\mathbb{F}_p[X]$, sont unitaires, irréductibles et deux à deux distincts, on a

$$\mathbb{F}_p[A] \sim \prod_{i=1}^{r} \mathbb{F}_p[X]/(P_i^{e_i})$$

et on voit que l'ordre k de A modulo p est lié à la décomposition de P modulo p. Dans notre cas, cette factorisation de $\bar{P}$ équivaut à la décomposition $(p) = (\mathbf{p}_1)^{e_1} \cdots (\mathbf{p}_r)^{e_r}$ de l'idéal (p) dans le corps de rupture de P, et le degré résiduel f_i de $\mathbf{p}_i$ est égal à $\deg P_i$ pour tout i. Ce un thèorémeest est dû essentiellement à Kummer.

Donnons l'exemple du cas $d = 3$ (le cas $d = 2$ se traite beaucoup plus simplement avec le symbole de Legendre). Les possibilités sont les suivantes

- $k \mid p-1$, alors $(p) = \mathbf{p}_1\mathbf{p}_2\mathbf{p}_3$, avec des $\mathbf{p}_i$ distincts et $f_1 = f_2 = f_3 = 1$,
- $k \mid p(p-1)$ et $k \nmid p-1$, alors $(p) = \mathbf{p}_1^2\mathbf{p}_2$, avec $\mathbf{p}_1 = \mathbf{p}_2$ ou $\mathbf{p}_1 \neq \mathbf{p}_2$ et $f_1 = f_2 = 1$,
- $k \mid p^2 - 1$ et $k \nmid p-1$, alors $(p) = \mathbf{p}_1\mathbf{p}_2$, avec $f_1 = 2$ et $f_2 = 1$,
- $k \mid p^3 - 1$ et $k \nmid p-1$, alors $(p) = \mathbf{p}_1$, avec $f_1 = 3$.

Le calcul de l'ordre de A permet donc de distinguer entre ces différents cas, il s'effectue en $O(d^2 \log p)$ opérations dans $\mathbb{F}_p[A]$. Cette question a été exposée — avec un langage légèrement différent — dans la note [4].

References

[1] J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Academic Press, London, 1967.
[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, Berlin, 1996.
[3] D.H. Lehmer, Computer technology applied to the theory of numbers, in: W.J. Leveque (Ed.), Studies in Number Theory, Prentice-Hall, Englewood Cliffs, NJ, 1969, pp. 117–151.
[4] M. Mignotte, Un algorithme sur la décomposition des polynômes dans un corps fini, C.R. Acad. Sci. Paris Ser. A (1975) 137–139.