International Mathematical Forum, 5, 2010, no. 10, 477 - 486

A Lecture on the Complexity of Factoring Polynomials over Global Fields

Ali Ayad

CEA LIST, Software Safety Laboratory
Point Courrier 94, Gif-sur-Yvette, F-91191 France
ayadali99100@hotmail.com
and
IRMAR, Campus de Beaulieu
Université Rennes 1, 35042, Rennes, France

Abstract

This paper provides an overview on existing algorithms for factoring polynomials over global fields with their complexity analysis from our experiments on the subject. It relies on our studies of the complexity of factoring parametric multivariate polynomials that is used for solving parametric polynomial systems in our PhD thesis. It is intended to be useful to two groups of people: those who wish to know what work has been done and those who would like to do work in the field. It contains an extensive bibliography to assist readers in exploring the field in more depth. The paper presents different methods and techniques used for computing irreducible factors of polynomials depending on the global field: $\mathbb{Q}$, finite fields or algebraic extensions. We describe also our algorithm for factoring parametric multivariate polynomials.

Mathematics Subject Classification (2000): 11Y16, 68W30, 11C08, 12D05

Keywords: Symbolic computations, complexity analysis, polynomial factorization, irreducible polynomials, parametric polynomials

1 Introduction

Polynomial factorization is one of the main problems in algebra and symbolic computations. It goes back to Newton, Gauss, Fermat, Kronecker, Hensel and others. Factoring polynomials reduces them to simple objects (i.e., polynomials with less degrees) that are easy to manipulate for symbolic computations as the computation of greatest common divisors of polynomials, the resolution of

algebraic systems of polynomial equations and the decomposition of algebraic varieties into irreducible components [12, 14, 27] (e.g., the irreducible factors of a polynomial define the irreducible components of the hypersurface defined by this polynomial). The factorization of polynomials combined with the Buchberger's algorithm [7, 17, 18] give also algorithms for primary decompositions of polynomial ideals [25, 26].

The paper surveys the complexity of existing algorithms for factoring polynomials over global fields going from the rational numbers field to algebraic extension fields. It is organized as follows: Section 2 is dedicated to the factorization of polynomials without parameters with coefficients in $\mathbb{Q}$ (Section 2.1), in finite fields (Section 2.2), in algebraic extensions (Section 2.3). Absolute factorization of polynomials is given in Section 2.4. Section 3 describes an algorithm for factoring parametric multivariate polynomials [1, 2].

2 Factoring polynomials without parameters

Let K be a global field and $f \in K[X_1, \ldots, X_n]$ be a multivariate polynomial in the variables $X_1, \ldots, X_n$ with coefficients in K. We say that f is irreducible in $K[X_1, \ldots, X_n]$ (i.e., irreducible over K) if there is no non-constant polynomials f_1, f_2 in $K[X_1, \ldots, X_n]$ such that $f = f_1 f_2$. It is well-known that f has a unique (up to factors in K^*) decomposition into a product of a finite number of irreducible polynomials $f_1, \ldots, f_s$ over K. This is called the factorization of f over K.

In this section, we are looking for efficient algorithms that compute the irreducible factors of f. There are many algorithms depending on the ground field K. For the complexity analysis aims, we suppose that the degree of f is less than an integer d.

2.1 Factoring over the field of rational numbers

Kronecker has factored univariate polynomials with integer coefficients by an algorithm with exponential complexity in d (see e.g [31, 42]).

Based on Berlekamp's algorithm [4, 5] and Hensel's Lemma (see e.g., [50, 45, 44, 14, 27, 49, 42]), Zassenhaus (see e.g., [50, 42]) has described an algorithm for factoring polynomials in $\mathbb{Z}[X]$ but also with exponential complexity in the size of the input polynomial.

The first algorithm of factorization of univariate polynomials aver $\mathbb{Q}$ with polynomial complexity in the size of the input polynomial was published in 1982 in [38] by A.K. Lenstra, H.W. Jr. Lenstra and L. Lovasz (the LLL-algorithm). The complexity bound of this algorithm is $d^{12} + d^9 \log^3 h$ where h is the binary length of the polynomial to be factored. It is based on the computation of minimal vectors of lattices.

In 1982, Chistov and Grigoryev have used the LLL-algorithm with a multivariate version of Hensel's Lemma to get a polynomial algorithm for factoring multivariate polynomials with coefficients in $\mathbb{Q}$ [11] (see also [12, 14, 27]). In the same year, Kaltofen [31, 32, 34] has presented a deterministic polynomial-time algorithm of reductions from multivariate to univariate integral polynomial factorization. This algorithm has polynomial complexity in d and the binary length of the input polynomial when the number of variables is fixed.

In 2002, Van Hoeij [30] has designed a new algorithm for factoring polynomials over $\mathbb{Q}$ by reducing the problem to a knapsack one using power sums. In 2004, Belabas [3] has generalized van Hoeij's algorithm to number fields, but these two papers stated no complexity bound.

Recently, in 2003, Gao [23] has described a probabilistic algorithm for factoring bivariate polynomials over $\mathbb{Q}$. This algorithm is based on the resolution of large linear systems and on the factorization of univariate polynomials over $\mathbb{Q}$. Its complexity is bounded by $\tilde{O}(d^5)$.

2.2 Factoring over finite fields

In the late 60s, Berlekamp [4, 5] has described a probabilistic algorithm which factorizes univariate polynomials with coefficients in a finite field with q elements by linear algebra methods. Its complexity bound is $O(d^3 \log q)$, being polynomial in the size of the input polynomial (see also [42]).

In 1982, Chistov and Grigoryev [11, 27, 14, 12] have presented polynomial-time algorithms for factoring multivariate polynomials with coefficients in a finite field $\mathbb{F}_q$. Their complexity bound is $(d^n \log q)^{O(1)}$. These algorithms are based on the computation of minimal vectors of lattices as in the LLL-algorithm [38].

In 1985, Von zur Gathen and Kaltofen [48] have got two polynomial-time algorithms for factoring polynomials in two variables with coefficients in $\mathbb{F}_q$: the first algorithm is probabilistic with complexity $(d \log q)^{O(1)}$ and the second algorithm is deterministic with complexity $(dq)^{O(1)}$. Later in the same year, A.K. Lenstra has obtained the same complexity bound [40] for factoring multivariate polynomials with coefficients in a finite field.

In 1995, Kaltofen and Shoup [35] have improved the complexity of the factorization of univariate polynomials with coefficients in $\mathbb{F}_q$. They found a complexity bound of $O(d^{1.815} \log q)$ by a family of probabilistic algorithms. Later in 1997 [36], they have given a lower bound of order $O(d \log^2 q)$.

In 2001, Flajolet et. al. [21] have obtained a complete analysis of a polynomial factorization algorithm over finite fields.

In 2002, Noro et. al. [46] have designed a practical way to factorize polynomials over finite fields using Gröbner bases [7, 17, 18] techniques.

Recently, in 2004, an improvement of the exponent $O(1)$ of these complexity

bounds is realized in [6] by a deterministic algorithm with complexity $\tilde{O}(d^{\omega+1})$ and a probabilistic algorithm with complexity $\tilde{O}(d^{\omega})$ for factoring bivariate polynomials with coefficients in $\mathbb{F}_q$ where ω is the linear algebra exponent [49] (i.e., the multiplication of two $n \times n$ matrices is done with n^{ω} elementary operations in the ground field where $2 < \omega \leq 3$ ($\omega \leq 2.376$ in [15])).

2.3 Factoring over algebraic extensions

When the ground field K is a finite extension of purely transcendental extension of its prime subfield (i.e., $K = H(T_1, \ldots, T_l)[\eta]$ where $H = \mathbb{Q}$ if $char(K) = 0$ and $H \supset \mathbb{F}_p$ is a finite extension of $\mathbb{F}_p$ if $char(K) = p > 0$, the variables $T_1, \ldots, T_l$ are algebraically independant over H and η is algebraic, separable over the field $H(T_1, \ldots, T_l)$), Chistov and Grigoryev [11, 27, 14, 12] have described a polynomial-time algorithm for factoring multivariate polynomials with coefficients in K.

When $K = \mathbb{Q}[\eta]$ where η is algebraic over $\mathbb{Q}$ with minimal polynomial $\phi \in \mathbb{Q}[Z]$ (where Z is a new variable). The factorization of a multivariate polynomial $f \in \mathbb{Z}[\eta][X_1, \ldots, X_n]$ is done also in polynomial-time in the size of f [39, 34, 37, 41]. The coefficients of the irreducible factors are represented by polynomials in η of degrees $< \deg(\phi)$. This complexity is bounded by $(h \deg(\phi) d^n)^{O(1)}$ where h is the maximal binary length of the coefficients of f in $\mathbb{Z}$.

2.4 Absolute factorization

A polynomial $f \in K[X_1, \ldots, X_n]$ is absolutely irreducible if it is irreducible over an algebraic closure $\overline{K}$ of K, this is equivalent to that f is irreducible over all algebraic extensions of K. The absolute factorization of f is its unique decomposition into a product of absolutely irreducible factors. Two strategies are adopted for the absolute factorization of polynomials:

2.4.1 Symbolic computations

This strategy aims to compute a primitive extension $K[\alpha]$ of K represented by the minimal polynomial of α over K that contains all coefficients of all the absolutely irreducible factors of f.

In 1981, Heintz and Sieveking [29] have given a first polynomial-time test for absolute factorization of polynomials.

In 1983, Chistov and Grigoryev [12] (see also [14]) have proposed for the first time a polynomial-time algorithm of reductions from absolute factorization to factorization over the ground field K. This algorithm is combined with another polynomial-time algorithm of factorization over K (where K is a finite extension of purely transcendental extension of its prime subfield as above) to

get a polynomial-time algorithm for absolute factorizations. The complexity of their algorithm is polynomial in d^{n^2}.

In 1985, Kaltofen [33] has computed the minimal polynomial of a given root of f in $\overline{K}$. This polynomial is in fact an absolutely irreducible factor of f.

In 1987 [19] and 1991 [20], Duval has used geometric methods on the hypersurface defined by f to get algorithms for its absolute factorization.

In 2003, Gao [23] has described a probabilistic algorithm for absolute factorizations of bivariate polynomials with coefficients in a field of characteristic zero or of characteristic $p > d(d-1)$. This algorithm is based on the resolution of large linear systems and on the factorization of univariate polynomials over the ground field. Its complexity is bounded by $\tilde{O}(d^5)$. This bound was improved later in 2007 by Chèze and Lecerf [9] (see also [8]). They have shown two algorithms: the first is deterministic with complexity $\tilde{O}(d^4)$ and the second algorithm is probabilistic with sub-quadratic complexity $\tilde{O}(d^{(\omega+3)/2})$ in the size d^2 of the input polynomial. These algorithms are implemented in Magma[1] and they are efficient in practice [8].

2.4.2 Numeric computations

Numeric computation strategy consists to compute an approximation of the coefficients of the absolutely irreducible factors of f when $K = \mathbb{Q}$. Let $f_1, \ldots, f_s$ be the absolutely irreducible factors of f in $\mathbb{Q}[X, Y]$ (i.e., the exact factors) and $\tilde{f}_1, \ldots, \tilde{f}_s \in \mathbb{R}[X, Y]$. We say that $f \approx \tilde{f}_1 \cdots \tilde{f}_s$ is an approximate absolute factorization of f with precision $\epsilon > 0$ if for all $1 \leq i \leq s$, the coefficients of $\tilde{f}_i$ are numeric approximations of those of f_i with precision ϵ, i.e., for all $1 \leq i \leq s$, $\| f_i - \tilde{f}_i \|_\infty < \epsilon$ where $\| g \|_\infty$ is the maximal absolute value of the coefficients of $g \in \mathbb{R}[X, Y]$.

Chèze and Galligo [10, 8] have established an algorithm which constructs exact factors from approximate factors. There are many other geometric algorithms that compute numeric approximate absolute factorization of bivariate polynomials with coefficients in $\mathbb{Q}$ [22, 16, 8, 24, 47, 10].

3 Factoring polynomials with parameters

Let K be a global field and $F \in K[u_1, \ldots, u_r][X_1, \ldots, X_n]$ be a parametric multivariate polynomial in the variables $X_1, \ldots, X_n$ with polynomial coefficients in the variables $u = (u_1, \ldots, u_r)$ (the parameters) over K. Our goal is to compute the absolute factorization of F uniformly for different values of the parameters

[1] `http://www.math.uvsq.fr/~lecerf/software/absfact/index.html`

in the set $\mathcal{P} = \overline{K}^r$ which we call the parameters space (see Example 3.1 and below). For the complexity analysis aims, we suppose that the degree of F w.r.t. $X_1, \ldots, X_n$ is less than d. In the sequel, let us adopt the following notation: for a polynomial $g \in K(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ and a value $a = (a_1, \ldots, a_r) \in \mathcal{P}$ of the parameters, we denote by $g^{(a)}$ the polynomial of $\overline{K}[X_1, \ldots, X_n]$ which is obtained by specialization of u by a in the coefficients of g if their denominators do not vanish on a, i.e., $g^{(a)} = g(a_1, \ldots, a_r, X_1, \ldots, X_n)$.

Example 3.1 *Let the following parametric bivariate polynomial*

$$F = (u^2 + v)X^2 + uXY + vX + uY + v \in \mathbb{Q}[u, v][X, Y]$$

One can decompose $\mathbb{C}^2$ *into three sets* $\mathcal{V}_1, \mathcal{V}_2$ *and* $\mathcal{V}_3$ *as follows:*

$$\left\{ \begin{array}{l} \mathcal{V}_1 = \{u^2 + v = 0\} \\ F = (X+1)(uY+v) \end{array} \right. , \left\{ \begin{array}{l} \mathcal{V}_2 = \{u^2 + v \neq 0,\ u \neq 0\} \\ F \text{ is absolutely irreducible} \end{array} \right. , \left\{ \begin{array}{l} \mathcal{V}_3 = \{u = 0, v \neq 0\} \\ F = v(X - C)(X - C^2) \end{array} \right.$$

This reads as follows: for any $(a, b) \in \mathcal{V}_1$*, the absolute factorization of* $F^{(a,b)}$ *is given by* $F^{(a,b)} = (X + 1)(aY + b)$*. For any* $(a, b) \in \mathcal{V}_2$*,* $F^{(a,b)}$ *is absolutely irreducible. For any* $(a, b) \in \mathcal{V}_3$*, there exists* c*, a cubic primitive root of the unity (i.e., a root of the polynomial* $\chi = C^3 - 1$ *where* C *is a new variable according to the representation below) such that* $F^{(a,b)} = b(X - c)(X - c^2)$ *is the absolute factorization of* $F^{(a,b)}$*.*

In 2004 [1] (see also [2]), we have described an algorithm which computes a finite partition of $\mathcal{P}$ into constructible sets $\mathcal{V}$ such that the absolute factorization of F is given uniformly in each constructible set $\mathcal{V}$, i.e., the algorithm computes s polynomials $G_1, \ldots, G_s \in K(C, u_1, \ldots, u_r)[X_1, \ldots, X_n]$ (where C is a new variable), and a polynomial $\chi \in K(u_1, \ldots, u_r)[C]$ which satisfy the following property:

- For any $a \in \mathcal{V}$, there exists $c \in \overline{K}$, a root of $\chi^{(a)} \in \overline{K}[C]$ such that the denominators of the coefficients of χ and G_j do not vanish on a and (c, a) respectively and the absolute factorization of $F^{(a)}$ is given by

$$F^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c,a)}, \quad G_j^{(c,a)} \text{ is absolutely irreducible.}$$

The parametric polynomial χ defines the extension of K where the coefficients of the factors belong to. In addition, the algorithm computes bounds on the degrees and the binary lengths of the output polynomials. Its complexity is single exponential in n, r and d. This algorithm is based on a parametric version of Hensel's Lemma and an algorithm of quantifier elimination in the theory of algebraically closed field [13] in order to reduce the problem of finding absolute irreducible factors to the problem of representing solutions of zero-dimensional parametric polynomial systems [28, 43].

4 Conclusion

In this paper, we have presented an overview on the complexity of factoring polynomials over several ground fields: $\mathbb{Q}$, finite fields and algebraic extension fields. We have shown algorithms for absolute factorization of polynomials by symbolic and numeric computations. Different methods for representing irreducible factors of polynomials are given with their complexity analysis for the parametric and the non-parametric case. In anyway, this paper reflects our point of view on the problem and is not considered as an exhaustive paper on the historic of the problem.

References

[1] A. Ayad, *Complexity bound of absolute factoring of parametric polynomials*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 316, Teor. Slozhn. Vychisl. **9**, 224 (2004), 5 - 29. Translated to Journal of Mathematical Sciences (N. Y.), **134**, No. 5 (2006), 2325 - 2339.

[2] A. Ayad, *Complexité de la résolution des systèmes algébriques paramétriques*, PhD thesis, University of Rennes 1, France, 2006.

[3] K. Belabas, *A relative van Hoeij algorithm over number fields*, Journal of Symbolic Computation, **37** (2004), 641 - 668.

[4] E.R. Berlekamp, *Factoring polynomials over finite fields*, Bell Systems Tech. J., **46** (1967), 1853 - 1859.

[5] E.R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp., **24** (1970), 713 - 735.

[6] A. Bostan, G. Lecerf, B. Salvy, Schost, B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, ISSAC 2004, Spain, 42 - 49.

[7] B. Buchberger, *Gröbner Bases: An algorithmic method in polynomial ideal theory*, in Multidimensional System Theory (N.K.Bose et. al., Eds), Reidel, Dordrecht (1985), 374 - 383.

[8] G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*. PhD thesis, University of Nice - Sophia-Antipolis, 2004.

[9] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, Journal of Complexity, **23**, Issue 3 (2007), 380 - 420.

[10] G. Chèze and A. Galligo, *From an approximate to an exact absolute polynomial factorization*, Journal of symbolic computation, **41**, No. 6 (2006), 682 - 696.

[11] A. Chistov, D. Grigoriev, *Polynomial-time factoring of the multivariable polynomials over a global field*, Preprint LOMI E-5-82, Leningrad, 1982.

[12] A.L. Chistov and D. Grigoryev, *Subexponential-time solving systems of algebraic equations*, I and II, LOMI Preprint, Leningrad, 1983, E-9-83, E-10-83.

[13] A. Chistov, D. Grigoriev, *Complexity of quantifier elimination in the theory of algebraically closed fields*, LNCS, **176** (1984), 17 - 31.

[14] A.L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math., **34**, No. 4 (1986), 1838 - 1882.

[15] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*, In proceedings of the Nineteenth Annual ACM Symposium on Theory of computing, 1987, 1 - 6.

[16] R. M. Corless, A. Galligo, I. S. Kotsireas and S. M. Watt, *A geometric-numeric algorithm for absolute factorization of multivariate polynomials*, ISSAC 2002, France, 37 - 45.

[17] D. Cox, J. Little and D. O'shea, *Ideals, Varieties and Algorithms*, Second Edition, Springer, 1997.

[18] D. Cox, J. Little and D. O'shea, *Using Algebraic Geometry*, Springer, 1998.

[19] D. Duval, *Une approche géométrique de la factorisation absolue de polynômes*. PhD Thesis: Diverses questions relatives au calcul formel avec des nombres algébriques, University of Grenoble 1, 1987, 71 - 104.

[20] D. Duval, *Absolute Factorization of Polynomials : A Geometric Approch*, SIAM Journal of Computing **20**, No. 1 (1991), 1 - 21.

[21] P. Flajolet, X. Gourdon, and D. Panario, *The complete analysis of a polynomial factorization algorithm over finite fields*, J. Algorithms, **40(1)** (2001), 37-81.

[22] A. Galligo and S. Watt, *A numerical absolute primality test for bivariate polynomials* , ISSAC'97, Maui, Hawaii, United States, 1997, 217 - 224.

[23] S. Gao, *Factoring multivariate polynomials via partial differential equations*, American Mathematical Society, **72**, Issue 242 (2003), 801 - 822.

[24] S. Gao, E. Kaltofen, J. May, Z. Yang and L. Zhi, *Approximate factorization of multivariate polynomials via differential equations*, ISSAC 2004, Spain, 167 - 174.

[25] H-G. Gräbe, *On Factorized Gröbner Bases*, In "Computer Algebra in Science and Engineering" (ed. Fleischer, Grabmeier, Hehl), World Scientific Singapore, 1995, 77 - 89.

[26] H-G. Gräbe, *Minimal Primary Decomposition and Factorized Gröbner Bases*, in J. AAECC, **8** (1997), 265 - 278.

[27] D. Grigoryev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations*, J. Sov. Math., **34**, No. 4 (1986), 1762 - 1803.

[28] D. Grigoryev and N. Vorobjov, *Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute*, Proc. ACM Intern. Conf. Symb and Algebraic Computations, Scotland, 2000, 137 - 145.

[29] J. Heintz and M. Sieveking, *Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables*, Proc. 1981 International Conference on Automata and Languages, Lecture Notes in Computer Science 11, Springer-Verlag (1981), 16 - 28.

[30] M. van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory, **95** (2002), 167 - 189.

[31] E. Kaltofen, *On the complexity of factoring polynomials with integer coefficients*. PhD thesis, Rensselaer Polytechnic Instit., Troy, N.Y., December 1982.

[32] E. Kaltofen, *Factorization of polynomials*, Computer algebra, Springer, Vienna, 1983, 95 - 113.

[33] E. Kaltofen, *Fast Parallel Absolute Irreducibility Testing*, J. Symbolic Computation **1** (1985), 57 - 67.

[34] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization*, SIAM J. Comput., **14(2)** (1985), 469 - 489.

[35] E. Kaltofen and V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, In Proc. 27th Annual ACM Symp. Theory Comput., New York, N.Y., 1995. ACM Press, 398 - 406.

[36] E. Kaltofen and V. Shoup, *Fast Polynomial Factorization Over High Algebraic Extensions of Finite Fields*, ISSAC'97, Maui, Hawaii, 184 - 188.

[37] S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput., **14** (1985), 184 - 195.

[38] A.K. Lenstra, H.W.Jr. Lenstra, L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261**, No. 4 (1982), 515 - 534.

[39] A. K. Lenstra, *Lattices and factorization of polynomials over algebraic number fields*, LNCS, Springer, Berlin, **144** (1982), 32 - 39.

[40] A.K. Lenstra, *Factoring multivariate polynomial over finite fields*, J. Comput. System Sci. **30**, No. 2 (1985), 235 - 248.

[41] A. K. Lenstra, *Factoring multivariate polynomials over algebraic number fields*, SIAM J. Comput. **16** (1987), 591 - 598.

[42] M. Mignotte and D. Stefanescu, *Polynomials An Algorithmic Approach*, Springer, 1999.

[43] A. Montes, *A new algorithm for discussing Gröbner basis with parameters*, J. of Symb. Comp., **33** (2002), 183 - 208.

[44] D.R. Musser, *Multivariate polynomial factorization*, J. of A.C.M. t. **197** (1975), 291 - 309.

[45] D.R. Musser, *Algorithms for polynomial factorization*. PhD thesis and TR **134**, Univ. of Wisconsin, 1971.

[46] M. Noro and K. Yokoyama, *Yet another practical implementation of polynomial factorization over finite fields*, In T. Mora, editor, Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. ISSAC'02, New York, 200 - 206.

[47] A. J. Sommese, J. Verschelde and C.W. Wampler, *Numerical factorization of multivariate complex polynomials*, Theoretical Comput. Sci. **315**, 2-3 (2004), 651 - 669.

[48] J. von zur Gathen, E. Kaltofen, *Factorization of multivariate polynomials over finite fields*, Math. Comp. **45**, No. 171 (1985), 251 - 261.

[49] J. von zur Gathen and J. Gerhard, *Modern Computer algebra*, Cambridge University Press 1999.

[50] H. Zassenhaus, *On Hensel factorization*, J. Number Theory, **1** (1969), 291 - 311.

Received: June, 2009