Journal of Number Theory 147 (2015) 549–589

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Higher Newton polygons and integral bases [☆]

Jordi Guàrdia [a], Jesús Montes [b,c], Enric Nart [d,*]

[a] Departament de Matemàtica Aplicada IV, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, Av. Víctor Balaguer s/n, E-08800 Vilanova i la Geltrú, Catalonia, Spain

[b] Departament de Ciències Econòmiques i Empresarials, Facultat de Ciències Socials, Universitat Abat Oliba CEU, Bellesguard 30, E-08022 Barcelona, Catalonia, Spain

[c] Departament de Matemàtica Econòmica, Financera i Actuarial, Facultat d'Economia i Empresa, Universitat de Barcelona, Av. Diagonal 690, E-08034 Barcelona, Catalonia, Spain

[d] Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia, Spain

ARTICLE INFO

Article history:
Received 30 October 2013
Accepted 23 July 2014
Available online 5 October 2014
Communicated by Michael E. Pohst

MSC:
primary 11R04
secondary 11Y40, 14G15, 14H05

Keywords:
Dedekind domain
Global field
Local field
Montes algorithm
Newton polygon
$\mathfrak{p}$-integral bases
Reduced bases

ABSTRACT

Let A be a Dedekind domain whose field of fractions K is a global field. Let $\mathfrak{p}$ be a non-zero prime ideal of A, and $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. The Montes algorithm factorizes a monic irreducible polynomial $f \in A[x]$ over $K_\mathfrak{p}$, and provides essential arithmetic information about the finite extensions of $K_\mathfrak{p}$ determined by the different irreducible factors. In particular, it can be used to compute a $\mathfrak{p}$-integral basis of the extension of K determined by f. In this paper we present a new and faster method to compute $\mathfrak{p}$-integral bases, based on the use of the quotients of certain divisions with remainder of f that occur along the flow of the Montes algorithm.

[☆] Partially supported by MTM2009-10359 and MTM2012-34611 from the Spanish MEC.

[*] Corresponding author.

E-mail addresses: guardia@ma4.upc.edu (J. Guàrdia), montes3@uao.es, jesus.montes@ub.edu (J. Montes), nart@mat.uab.cat (E. Nart).

http://dx.doi.org/10.1016/j.jnt.2014.07.027
0022-314X/© 2014 Elsevier Inc. All rights reserved.

0. Introduction

One of the basic ingredients in computational algebraic number theory is the factorization of polynomials over p-adic fields. Classical strategies allow to derive from this problem the computation of integral bases, which is the starting point of most of the algorithms related to maximal orders in number fields.

We introduced in [7] a different approach to ideal arithmetic in number fields based on the decomposition of rational primes as provided by the Montes algorithm [5,8]. This approach included an *OM method* for the computation of p-integral bases which is significantly faster than the traditional methods, most of them based on variants of the Round 2 and Round 4 routines [2,3,10,18,22,23].

In this paper we present an alternative faster method based on the use of *quotients of ϕ-adic expansions*, which are directly provided by the Montes algorithm. This idea goes back to a construction of integral bases by W.M. Schmidt for certain subrings of function fields [19].

Our method works in a more general setting. Let A be a Dedekind domain whose field of fractions K is a global field. Let $\mathfrak{p}$ be a non-zero prime ideal of A, and $\pi \in A$ a local generator of $\mathfrak{p}$. Let $K_\mathfrak{p}$ be the completion of K with respect to the $\mathfrak{p}$-adic topology. Let $f \in A[x]$ be a monic irreducible separable polynomial of degree n. For $\theta \in K^{\mathrm{sep}}$ a root of f let $L = K(\theta)$ be the finite separable extension of K generated by θ and B the integral closure of A in L.

Following a program suggested by Ø. Ore [17] and developed by S. MacLane in the context of valuation theory [13,14], the Montes algorithm computes an *OM representation* of every prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$. This computational object supports several data and operators linked to some irreducible factor F of f in $K_\mathfrak{p}[x]$. Along the flow of the algorithm, some polynomials $\phi \in A[x]$ are constructed as a kind of partial approximations to F. The ϕ-expansions of f provide the necessary data to build higher order Newton polygons of f from which new and better approximations are deduced. As a by-product of the computation of any ϕ-expansion $f(x) = \sum_{0\le s} a_s(x)\phi(x)^s$, several quotients are obtained:

$$f = \phi Q_1 + a_0, \quad Q_1 = \phi Q_2 + a_1, \quad \ldots$$

For each quotient Q, the highest exponent μ such that $Q(\theta)/\pi^\mu$ is $\mathfrak{p}$-integral can be read in the OM representation (Theorem 3.3, Corollary 3.7). In Section 4, we construct integral bases of the local extensions $L_\mathfrak{P}/K_\mathfrak{p}$ with adequate products of these quotients. In contrast with the former OM method, these elements are $\mathfrak{p}$-integral (globally integral if A is a PID) and not only $\mathfrak{P}$-integral. In Section 5 we use these $\mathfrak{p}$-integral elements to build a $\mathfrak{p}$-integral basis (Theorem 5.15).

This *method of the quotients* has two significant advantages with respect to the former OM method and all classical methods:

(1) It yields $\mathfrak{p}$-*reduced* bases. For instance, let $L = \mathbb{F}(t, x)$ be the function field of a curve C over a finite field $\mathbb{F}$, defined by an equation $f(t, x) = 0$, which is separable over