von zur Gathen, Joachim

Hensel and Newton methods in valuation rings. (English) Zbl 0581.13001

Math. Comput. 42, 637-661 (1984).

Hensel and Newton methods have received quite a lot of attention in algebraic computing. We present them in their natural framework, that of valuation rings. The Hensel method deals with factorization of polynomials, the Newton method with zeros of polynomials over the given valuation ring. Both methods take an approximate solution and produce a new approximation which is better with respect to the given valuation.

The Hensel method presented in section 2 describes a lifting of an approximate factorization of a given polynomial over a valuation ring, where the factors are approximately relatively prime. It results in two choices of an iterative procedure, one with linear and one with quadratic convergence behavior. It allows us to describe the factorization of certain polynomials that are not squarefree over the residue class field, a case not covered by the usual formulation.

In section 3, we present a Newton method for solving differential equations for formal power series in several variables, in the general case of systems of nonlinar partial differential equations. This includes the case of a system of algebraic equations. One obtains a simple condition which provides an iterative procedure to compute a solution. In section 4, we discuss an important recently discovered tool for factoring polynomials: computing short vectors in modules over (valuation) rings. This tool has been introduced by *A. K. Lenstra*, *H. W. Lenstra* jun. and *L. Lovász* [Math. Cent., Amst., Afd. Inf. IW 195/82 (1982; Zbl 0477.68043)] for factoring univariate integer polynomials.

We present a short vector algorithm in the cases of non-Archimedean valuations. This yields, in the final section, an algorithm for factoring univariate polynomials over a ring with sufficient valuations. Special cases of this algorithm include univariate polynomials over $\mathbb{Q}$ and bivariate polynomials over a finite field.

MSC:

13-04	Software, source code, etc. for problems pertaining to commutative algebra	Cited in **11** Documents
13F15	Commutative rings defined by factorization properties (e.g., atomic, factorial, half-factorial)	
68Q25	Analysis of algorithms and problem complexity	
13B25	Polynomials over commutative rings	
68W99	Algorithms in computer science	

Keywords:

Hensel method; factorization of polynomials; Newton method; zeros of polynomials over; univariate polynomials; bivariate polynomials

Full Text: DOI