de Weger, B. M. M.

Algorithms for diophantine equations. (English) Zbl 0687.10013

CWI Tract, 65. Amsterdam: Centrum voor Wiskunde en Informatica. viii, 212 p. Dfl. 33.00 (1989).

The book is an updated version of the author's excellent Ph.D. thesis written in 1987. The purpose of it is to give a systematic, computer oriented overview of certain algorithms, applicable for the complete resolution of several types of exponential and polynomial diophantine equations. The algorithms are based on the combination of Baker's method with a numerical reduction procedure discovered originally by *A. Baker* and *H. Davenport* [Q. J. Math., Oxf. II. Ser. 20, 129–137 (1969; Zbl 0177.06802)]. In the book several new and useful variants of this method are given. The algorithms presented are illustrated with interesting numerical examples. At the end of the book an update list of references is given on the theory and practical solution of the equations involved.

Chapter 1 is an introductory explanation of Baker's method, its p-adic analogue and the diophantine approximation techniques, frequently used in the book.

Chapter 2 gives the necessary basics from algebraic number theory and the estimates of Waldschmidt, Schinzel and Yu for linear forms in logarithms of algebraic numbers.

Chapter 3 is a detailed description of the computational methods for the reduction of the large upper bounds obtained by Baker's method for the solutions of diophantine equations. This chapter explains among others the use of the continued fraction algorithm, the lattice basis reduction algorithm of *A. Lenstra*, *H. Lenstra* and *L. Lovász* [Math. Ann. 261, 515–534 (1982; Zbl 0488.12001)], the Fincke-Pohst algorithm for finding short lattice vectors [*U. Fincke* and *M. Pohst*, Math. Comput. 44, 463–471 (1985; Zbl 0556.10022)], and the Davenport lemma with its generalizations.

Chapter 4 is devoted to the equation

$$G_n = wp_1^{m_1} \cdots p_s^{m_s} \quad \text{in } n \in \mathbb{N}, \quad 0 \leq m_1, \dots, m_s \in \mathbb{Z}$$

where G_n is a second order linear recurrence sequence, w is a given positive integer and $p_1, \dots, p_s$ are prime numbers. As an application, the generalized Ramanujan-Nagell equation

$$x^2 + k = p_1^{z_1} \cdots p_s^{z_s} \quad \text{in } x \in \mathbb{N}, \quad 0 \leq z_1, \dots, z_s \in \mathbb{Z}$$

is studied (with a fixed integer k).

In the following let S denote the set of integers composed of a finite number of prime numbers.

In Chapter 5 the equation

$$0 < x - y < y^\delta \quad \text{in } x, y \in S$$

is solved ($0 < \delta < 1$ is fixed). The numerical example given in this chapter extends a result of *R. J. Stroeker* and *R. Tijdeman* [Computational methods in Number Theory 2, Math. Cent. Tracts 155, 321–369 (1982; Zbl 0521.10013)].

In Chapter 6 S-unit equations of the type $x + y = z$, $x, y, z \in S$ are discussed. These equations are essential for several types of exponential and polynomial diophantine equations. The results of Chapter 5 are used here. The numerical example stated in the chapter gives interesting information about the Oesterle-Masser conjecture (abc conjecture).

In Chapter 7 the resolution of the equation $x + y = z^2$, $x, y \in S$, $z \in \mathbb{N}$, (x, y) square-free is explained, which has applications in arithmetic algebraic geometry.

Finally, in Chapter 8 the Thue equations $F(x, y) = m$ in $x, y \in \mathbb{Z}$ are examined, where F is an irreducible binary form of degree ≥ 3 and m is a non-zero integer. Two quartic Thue equations are solved completely, which are applied to find all integer points on an elliptic curve.

Reviewer: István Gaál (Debrecen)

MSC:

11Y50 Computer solution of Diophantine equations
11D61 Exponential Diophantine equations
11-02 Research exposition (monographs, survey articles) pertaining to number theory
11D41 Higher degree equations; Fermat's equation
11D59 Thue-Mahler equations
11J86 Linear forms in logarithms; Baker's method

Keywords:

computer resolution of diophantine equations; computational number theory; exponential equations; polynomial equations; algorithms; Baker's method; practical solution; linear forms in logarithms of algebraic numbers; computational methods; continued fraction algorithm; lattice basis reduction algorithm; Fincke-Pohst algorithm; short lattice vectors; Davenport lemma; generalized Ramanujan-Nagell equation; S-unit equations; Oesterle-Masser conjecture; abc conjecture; Thue equations; quartic Thue equations