BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 37, Number 2, Pages 207–208
S 0273-0979(99)00861-7
Article electronically published on December 21, 1999

The algorithmic resolution of Diophantine equations, by Nigel P. Smart, London Mathematical Society Student Texts 41, Cambridge University Press, Cambridge, 1998, xvi+ 243 pp., $26.95, ISBN 0 521 64633 2 (paperback)

There are only a few books on a subject close to that of this book, namely Mordell's book *Diophantine Equations*, which appeared in 1969, and De Weger's tract *Algorithms for Diophantine Equations*, published twenty years later, in 1989. Mordell's book is not exactly "algorithmic", in contrast with De Weger's.

As clearly indicated in the Introduction, "this is not a theoretical book but a practical one." And, all through the book, the author gives very precise practical remarks and indicates the limits of the currently known algorithms aimed to solve some types of diophantine equations.

The book is divided into three parts. Part 1 involves the study of the basic techniques used in almost all cases: p–adic numbers, the use of curves of genus zero and the application of the famous LLL–algorithm of Lenstra, Lenstra and Lovász. The section on p–adic numbers contains Strassmann's theorem and examples where it enables us to solve a diophantine equation completely, and also where it does not lead to a complete conclusion, but just gives an upper bound on the number of solutions. I quote this example because it shows the constant desire of the author to show what happens in practice with concrete examples when we apply some theoretical result. Of course, as in de Weger's thesis, the LLL–algorithm plays a central role in the complete resolution of many diophantine equations, and thus it is presented in detail. Its applications are given with several explicit examples, in particular applications to linear forms in real, complex and p–adic numbers.

Part 2 is first devoted to Baker's theory: the theory of lower bounds for linear forms in logarithms of algebraic numbers, in the complex case as well as in the p–adic case (the elliptic case appears in the third part). Then this part contains the well-known applications to Thue-Mahler equations (Chapter 7), S–unit equations (Chapter 8), and also some special forms in several variables (triangulary connected decomposable forms and discriminant form equations).

The third and last part deals with methods for finding integral and rational points on curves such as elliptic curves, hyperelliptic and superelliptic curves. This part contains a study of the methods to find a complete set of generators of the Mordell-Weil group of an elliptic curve. Chapter 14 presents the recent generalizations of the methods for elliptic curves to curves of higher genus, in particular hyperelliptic curves; the author treats the link with the jacobian variety of a curve of genus greater than one. The final chapter gives some information on special equations like Fermat's and Catalan's.

It is a real pleasure to read this book, mainly because the author gives many examples and many practical remarks concerning the effective solution of diophantine equations. The examples can be followed with the help of a computer, and much information is given concerning the different usable packages. There are also practical exercises at the end of each chapter.

2000 *Mathematics Subject Classification.* Primary 11D45, 11Y50.

There is only one remark with which I do not completely agree, and it is the following (which appears in Appendix A): "You should consider the use of linear form results in two or three logarithms as nothing but an algorithmic optimization. ... In fact in practice we will still need to use LLL to reduce the upper bounds so very little is gained from the use of such results." This remark is completely correct when one studies a given diophantine equation of fixed degree, for example a Thue equation. But things change completely when you want to solve a complete family of Thue equations: in practice it is not at all the same to treat individually 10^6 equations (which is the case with Thomas' example of cubic Thue equations, a bound obtained using special results on linear forms in two logarithms) instead of something like 10^{13}, which would result from a general estimate in Baker's theory. Another example is Catalan's equation, $x^p - y^q = \pm 1$ with $q > p$. Here we know (using again special results on linear forms with two logarithms) that $q < p^2$ for $p > 10^5$, and these estimates allow us to prove that for $p < 10^5$ there is no solution except $3^2 - 2^3 = 1$.

I want to conclude that this is a very attractive book, full of concrete information, which gives a very clear and lucid view of the current knowledge on the resolution of diophantine equations.

Maurice Mignotte
Universite Louis Pasteur
E-mail address: mignotte@math.u-strasbg.fr