10[11-02, 11Dxx]—*The algorithmic resolution of Diophantine equations*, by Nigel P. Smart, Cambridge University Press, New York, NY, 1999, xvi+243 pp., 23 cm, hardcover, $69.95, softcover $26.95

1. Introduction

A hundred years has passed since Hilbert posed his tenth problem: whether there exists an algorithm to determine if a given Diophantine equation has finitely or infinitely many solutions. By any reasonable measure, Hilbert would be pleased with the progress made in the last century. Although it has since been shown by Matijasevič that the general problem is undecidable, there have been significant advances on these problems for many classes of Diophantine equations. The most notable along these lines include the pioneering work of Thue and later work by Siegel and Roth on Diophantine approximation of algebraic numbers and its application to bivariate homogeneous form equations, the finite basis theorem for elliptic curves of Mordell and Weil, Baker's results on linear forms in the logarithms of algebraic numbers. Tijdeman's application of Baker's method to Catalan's equation, the results of Győry and later Evertse on S-unit equations, Schmidt's subspace theorem, Falting's proof of the Mordell conjecture, and without question the most notable being Wiles' proof that all semi-stable elliptic curves over the rational numbers are modular, yielding a proof of Fermat's Last Theorem.

Given the apparent renaissance of this subject area in modern times, together with the development of sophisticated computing technology, it is natural to consider many of these problems from an algorithmic perspective. In particular, if a given Diophantine equation is known to have only finitely many solutions, then one may attempt to construct an algorithm which will find all of the solutions. This is precisely what Smart's book is all about.

The author describes his text as a recipe book for solving Diophantine equations. This is perhaps inspired by the fundamental thesis of de Weger, and also perhaps by the lack of textbooks on this subject, especially given the outstanding developments in recent years. This book is long overdue, and the author has succeeded in producing a valuable asset for the shelf of anyone interested in learning about solving Diophantine equations. The only prerequisite for this book is some basic algebraic number theory, and so it would be suitable as a graduate textbook. This reviewer would certainly recommend it as such, given that the author has included many exercises and worked examples. In fact, the examples go a long way in making the book a success.

The content is based on fundamental theorems arising from Baker's work on estimates for linear forms in the logarithms of algebraic numbers, the p-adic case by Yu, and the elliptic case by David. Armed with this machinery, there are large classes of Diophantine equations for which there exist computable upper bounds for the size of solutions. The primary examples of these include bivariate homogeneous form equations, bivariate equations whose curve $F(x, y) = 0$ defines a curve of genus one, and superelliptic Diophantine equations $y^n = P(x)$. Unfortunately, the upper bounds deduced from Baker's theory are, in most cases, much too large for a computer to search for small solutions. Thus, a technique first devised by Baker and Davenport, and later refined by de Weger using methods from the geometry of numbers via lattice basis reduction, can be employed to reduce the upper bounds by an order of magnitude. In many cases this procedure can be iterated sufficiently

many times to deduce an upper bound for the original problem which is amenable to a computer search for all solutions.

The text begins with a historical perspective on the subject of Diophantine equations, with reference to some of the well-known topics that have shaped the subject as we now know it. Fermat receives enormous coverage, not only in relation to the Last Theorem, but also for his observation concerning the problem of integer factorization and his method of infinite descent. This immediately indicates the author's desire to incorporate algorithms into his presentation. A discussion on this topic is the content of the next section, and some words concerning computational complexity attempt to bring the reader into the mindset of a computational number theorist. The introductory chapter finishes off with an abstract description of Diophantine equation, and then a concrete example of one: the elliptic curve $Y^2 = X^3 - 4$. A nonalgorithmic proof that $(X, Y) = (5, \pm 11)$ and $(2, \pm 2)$ constitute all of the integer solutions to this equation is provided.

Part I of the book discusses a smattering of topics, some being in preparation for the main topics of the book and others of independent interest. Chapter Two discusses local theory: p-adic numbers and their extensions, p-adic numerical analysis, Hensel's lemma, the Newton–Raphson method in this context, and p-adic power series. These topics are used in the subsequent chapter where one is shown how to use local methods to solve some types of Diophantine equations. The method of Skolem is used to solve the equation $X^4 - 2Y^4 = \pm 1$. The author briefly covers the Hasse (Local-Global) principle, and Selmer's famous example $3X^3 + 4X^3 + 5X^3 = 0$. The chapter ends on an algorithmic note, as the author discusses the concept of sieving as it applies to finding (or rather ruling out) small solutions to Diophantine equations of the shape $y^2 = P(x)$. This will prove to be a useful tool, required for some of the algorithms in the later chapters. Chapter Four is devoted to solving ternary quadratic forms, with reference to local and global conditions for solvability, along with a sieving algorithm to find small solutions. In Chapter Five we finally arrive at the machinery which provides the basis for all of the recipes in this book. Methods from Diophantine approximation and the geometry of numbers are presented clearly and in considerable detail. In particular, the theory of continued fractions, approximation lattices, the lattice basis reduction method of Lenstra, Lenstra and Lovász, and its integer variant by de Weger are the topics of this chapter. Some important applications of these topics are presented in the next and final chapter of Part I. In particular, the theoretical basis for de Weger's reduction procedure via approximation of linear forms is described in the global and local cases, with details given for both the homogeneous and inhomogeneous cases. This is a crucial part of the book, and the author does well by providing a very explicit example to illuminate the procedure.

Of the three parts of the book, Part II is, in the reviewer's opinion, the most essential. Through the work of de Weger, Stroeker, Tzanakis and others, there have been significant developments in recent years of techniques which use linear forms in logarithms to deduce upper bounds for Diophantine equations, and then lattice basis reduction methods to lower these upper bounds. Chapter Seven provides a detailed description of how these methods apply to Thue equations (bivariate homogeneous Diophantine equations of the form $F(x, y) = 0$). The presentation is clear, and the examples exhibit the method of approximation lattices and lattice basis reduction very well. The author even describes a recent method due to Bilu and Hanrot, which lends itself to the complete solution of higher degree Thue

equations. In Chapter Eight, these methods are applied to Thue–Mahler equations. A general description of the methodology is presented along with the method as it applies to the specific example $X^3 - X^2Y + XY^2 + Y^3 = \pm 11^s$. In Chapter Nine the methods are applied to the more general problem of S-unit equations. Also, a sieving procedure for the determination of small solutions to S-unit equations is described. The problem of solving S-unit equations has developed into an important area of study within Diophantine approximation, with the pioneering work of Győry and Evertse. The myriad of applications of this pursuit are described at the end of Chapter Nine, and on into Chapter 10 and 11: triangularly connected decomposable form equations, discriminant form equations, and index form equations. Thue equations are a very special case of all of these. Complete algorithms for solving all of these types of Diophantine equations are described in considerable detail, along with many examples and exercises.

The last part of the book covers the topic of elliptic curves, with the primary goal of determining all integer points on an elliptic curve. The author provides a fairly detailed expository of the Mordell–Weil theorem, along with the computation of 2-Selmer groups, and the conjecture of Birch and Swinnerton-Dyer. The main topic in Part III is Chapter 13, in which all integer points on an elliptic curve are determined using David's estimates for linear forms in elliptic logarithms, and reduction techniques similar in nature as those described in earlier chapters. The author once again succeeds in presenting the method very clearly with illuminating examples. The final chapter superficially covers an assortment of topics that the reader may wish to go off and see more of via the literature provided. These include Faltings' famous theorem on the finiteness of the number of rational points on curves of genus two, an effective method going back to Chabauty for finding rational points on such curves via their Jacobians (the reader should be aware that the subject of Diophantine analysis fails from the shortcoming of an almost complete lack of effective methods for finding all integer points on a curve of genus $g > 1$). Unfortunately, some recent work of Bruin on this particular topic did not manage to make it into the book. The chapter is completed by some remarks on Fermat curves, and Catalan's equation. Two appendices are provided for the reader, with the first of these providing the theoretical basis for the book. In particular, precise estimates for linear forms in complex logarithms of algebraic numbers due to Baker and Wustholz are given, along with the p-adic version due to Yu, and David's result for linear forms in elliptic logarithms.

The basic philosophy in this book is to follow a mathematical recipe, combining theory and computation, to solve a single Diophantine equation. There are many examples provided which convey the techniques very nicely. One should keep in mind that it can be the case that a given Diophantine problem, or classes thereof, can be completely solved without the brute force of a computer. For example, results of Ljunggren and Cohn have completely solved the family of elliptic curves given by quartic models of the form $X^4 - dY^2 = 1$ without perhaps a single keystroke on a computer. Nevertheless, the main point of Smart's book is to exhibit how the reduction techniques of de Weger can be used to minimize the required computation, which is clearly worthwhile. There is also a surprising absence of reference to recent work by Coppersmith, in which lattice basis reduction methods are used to find small solutions to certain classes of Diophantine equations with applications to integer factorization.

The Algorithmic resolution of Diophantine equations is full of interesting and fundamental mathematics. It has the advantage of holding both the theoretical and the computational mathematician's attention. The chapters do seem to be presented at varying depths, and there is some discrepancy as to precisely who the author is writing to, but overall the presentation is certainly motivating.

P. G. Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada
K1N-6N5
E-mail address: gwalsh@mathstat.uottawa.ca