Cambridge studies in advanced mathematics 146

Unit Equations in Diophantine Number Theory

JAN-HENDRIK EVERTSE
KÁLMÁN GYŐRY

Unit Equations in Diophantine Number Theory

JAN-HENDRIK EVERTSE
Universiteit Leiden

KÁLMÁN GYŐRY
Debreceni Egyetem, Hungary

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107097605

First published 2015

Printed in the United Kingdom by Clays, St Ives plc

A catalogue record for this publication is available from the British Library

ISBN 978-1-107-09760-5 Hardback

CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS 146

UNIT EQUATIONS IN DIOPHANTINE NUMBER THEORY

Diophantine number theory is an active area that has seen tremendous growth over the past century, and in this theory unit equations play a central role. This comprehensive treatment is the first volume devoted to these equations. The authors gather together all the most important results and look at many different aspects, including effective results on unit equations over number fields, estimates on the number of solutions, analogues for function fields, and effective results for unit equations over finitely generated domains. They also present a variety of applications. Introductory chapters provide the necessary background in algebraic number theory and function field theory, as well as an account of the required tools from Diophantine approximation and transcendence theory. This makes the book suitable for young researchers as well as for experts who are looking for an up-to-date overview of the field.

Jan-Hendrik Evertse works at the Mathematical Institute of Leiden University. His research concentrates on Diophantine approximation and applications to Diophantine problems. In this area he has obtained some influential results, in particular on estimates for the numbers of solutions of Diophantine equations and inequalities. He has written more than 75 research papers and co-authored one book with Bas Edixhoven entitled *Diophantine Approximation and Abelian Varieties*.

Kálmán Győry is Professor Emeritus at the University of Debrecen, a member of the Hungarian Academy of Sciences and a well-known researcher in Diophantine number theory. Over his career he has obtained several significant and pioneering results, among others on unit equations, decomposable form equations, and their various applications. His results have been published in one book and 160 research papers. Győry is also the founder and leader of the number theory research group in Debrecen, which consists of his former students and their students.

CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing visit www.cambridge.org/mathematics.

Already published

109 H. Geiges *An introduction to contact topology*
110 J. Faraut *Analysis on Lie groups: An introduction*
111 E. Park *Complex topological K-theory*
112 D. W. Stroock *Partial differential equations for probabilists*
113 A. Kirillov, Jr *An introduction to Lie groups and Lie algebras*
114 F. Gesztesy *et al. Soliton equations and their algebro-geometric solutions, II*
115 E. de Faria & W. de Melo *Mathematical tools for one-dimensional dynamics*
116 D. Applebaum *Lévy processes and stochastic calculus (2nd Edition)*
117 T. Szamuely *Galois groups and fundamental groups*
118 G. W. Anderson, A. Guionnet & O. Zeitouni *An introduction to random matrices*
119 C. Perez-Garcia & W. H. Schikhof *Locally convex spaces over non-Archimedean valued fields*
120 P. K. Friz & N. B. Victoir *Multidimensional stochastic processes as rough paths*
121 T. Ceccherini-Silberstein, F. Scarabotti & F. Tolli *Representation theory of the symmetric groups*
122 S. Kalikow & R. McCutcheon *An outline of ergodic theory*
123 G. F. Lawler & V. Limic *Random walk: A modern introduction*
124 K. Lux & H. Pahlings *Representations of groups*
125 K. S. Kedlaya *p-adic differential equations*
126 R. Beals & R. Wong *Special functions*
127 E. de Faria & W. de Melo *Mathematical aspects of quantum field theory*
128 A. Terras *Zeta functions of graphs*
129 D. Goldfeld & J. Hundley *Automorphic representations and L-functions for the general linear group, I*
130 D. Goldfeld & J. Hundley *Automorphic representations and L-functions for the general linear group, II*
131 D. A. Craven *The theory of fusion systems*
132 J.Väänänen *Models and games*
133 G. Malle & D. Testerman *Linear algebraic groups and finite groups of Lie type*
134 P. Li *Geometric analysis*
135 F. Maggi *Sets of finite perimeter and geometric variational problems*
136 M. Brodmann & R. Y. Sharp *Local cohomology (2nd Edition)*
137 C. Muscalu & W. Schlag *Classical and multilinear harmonic analysis, I*
138 C. Muscalu & W. Schlag *Classical and multilinear harmonic analysis, II*
139 B. Helffer *Spectral theory and its applications*
140 R. Pemantle & M. C. Wilson *Analytic combinatorics in several variables*
141 B. Branner & N. Fagella *Quasiconformal surgery in holomorphic dynamics*
142 R. M. Dudley *Uniform central limit theorems (2nd Edition)*
143 T. Leinster *Basic category theory*
144 I. Arzhantsev, U. Derenthal, J. Hausen & A. Laface *Cox rings*
145 M. Viana *Lectures on Lyapunov exponents*
146 J.-H. Evertse & K. Győry *Unit equations in Diophantine number theory*
147 A. Prasad *Representation theory*
148 S. R. Garcia, J. Mashreghi & W. T. Ross *Introduction to model spaces and their operators*

Preface

Diophantine number theory (the study of Diophantine equations, Diophantine inequalities and their applications) is a very active area in number theory with a long history. This book is about *unit equations*, a class of Diophantine equations of central importance in Diophantine number theory, and their applications. Unit equations are equations of the form

$$a_1x_1 + \cdots + a_nx_n = 1$$

to be solved in elements $x_1, \ldots, x_n$ from a finitely generated multiplicative group Γ, contained in a field K, where $a_1, \ldots, a_n$ are non-zero elements of K. Such equations were studied originally in the cases where the number of unknowns $n = 2$, K is a number field and Γ is the group of units of the ring of integers of K, or more generally, where Γ is the group of S-units in K. Unit equations have a great variety of applications, among others to other classes of Diophantine equations, to algebraic number theory and to Diophantine geometry.

Certain results concerning unit equations and their applications covered in our book were already presented, mostly in special or weaker form, in the books of Lang (1962, 1978, 1983), Győry (1980b), Sprindžuk (1982, 1993), Evertse (1983), Mason (1984), Shorey and Tijdeman (1986), de Weger (1989), Schmidt (1991), Smart (1998), Bombieri and Gubler (2006), Baker and Wüstholz (2007) and Zannier (2009), and in the survey papers of Evertse, Győry, Stewart and Tijdeman (1988b), Győry (1992a, 1996, 2002a, 2010) and Bérczes, Evertse and Győry (2007b).

In 1988, we wrote, together with Stewart and Tijdeman, the survey Evertse, Győry, Stewart and Tijdeman (1988b) on unit equations and their applications giving the state of the art of the subject at that time. Since then, the theory of unit equations has been greatly expanded. In the present book we have

tried to give a comprehensive and up-to-date treatment of unit equations and their applications. We prove effective finiteness results for unit equations in two unknowns, describe practical algorithms to solve such equations, give explicit upper bounds for the number of solutions, discuss analogues of unit equations over function fields and over finitely generated domains, and present various applications. The proofs of the results concerning unit equations are mostly based on the very powerful Thue–Siegel–Roth–Schmidt theory from Diophantine approximation and Baker's theory from transcendence theory. We note that there are other important methods and applications, some discovered very recently, that deserve a detailed discussion, but to which we could pay only little or no attention due to lack of time and space.

The present book is the first in a series of two. The second book, titled *Discriminant Equations in Diophantine Number Theory*, also published by Cambridge University Press, is about polynomials and binary forms of given discriminant, with applications to algebraic number theory, Diophantine approximation and Diophantine geometry. There, we will apply the results from the present book. The contents of these two books are an outgrowth of research, done by the two authors since the 1970s.

The present book is aimed at anybody (graduate students and experts) with basic knowledge of algebra (groups, commutative rings, fields, Galois theory) and elementary algebraic number theory. For convenience of the reader, in part I of the book we have provided some necessary background.

Acknowledgments

We are very grateful to Yann Bugeaud, Andrej Dujella, István Gaál, Rafael von Känel, Attila Pethő, Michael Pohst, Andrzej Schinzel and two anonymous referees for carefully reading and critically commenting on some chapters of our book, to Csaba Rakaczki for his careful typing of a considerable part of this book, and to Cambridge University Press, in particular David Tranah, Sam Harrison and Clare Dennison, for their suggestions for and assistance with the final preparation of the manuscript.

The research of the second named author was supported in part by Grants 100339 and 104208 from the Hungarian National Foundation for Scientific Research (OTKA).

Summary

We start with a brief historical overview and then outline the contents of our book. Thue (1909) proved that if $F \in \mathbb{Z}[X, Y]$ is a binary form (i.e., a homogeneous polynomial) of degree at least 3 which is irreducible over $\mathbb{Q}$ and if δ is a non-zero integer, then the equation

$$F(x, y) = \delta \text{ in } x, y \in \mathbb{Z}$$

(nowadays called a *Thue equation*) has only finitely many solutions. To this end, Thue developed a very original Diophantine approximation method concerning the approximation of algebraic numbers by rationals, which was extended later by Siegel, Dyson, Gelfond and Roth.

Thue's result was generalized by Siegel (1921) as follows. Let K be an algebraic number field of degree d with ring of integers O_K, let $F \in O_K[X, Y]$ be a binary form of degree $n > 4d^2 - 2d$ such that $F(1, 0) \neq 0$ and $F(X, 1)$ has no multiple zeros, and let δ be a non-zero element of O_K. Then the equation

$$F(x, y) = \delta \text{ in } x, y \in O_K$$

has only finitely many solutions. This has the following interesting consequence, which was not stated explicitly by Siegel, but which was implicitly proved by him. Denote by O_K^* the group of units of O_K. Let a_1, a_2 be non-zero elements of the number field K. Then the equation

$$a_1 x_1 + a_2 x_2 = 1 \tag{1}$$

has only finitely many solutions in $x_1, x_2 \in O_K^*$. To prove this, choose an integer $n > 4d^2 - 2d$. By Dirichlet's Unit Theorem, the group O_K^* is finitely generated, and thus, any solution $x_1, x_2 \in O_K^*$ of (1) can be written as $x_i = \beta_i \varepsilon_i^n$ for $i = 1, 2$ with $\beta_i, \varepsilon_i \in O_K^*$, such that β_i may assume only finitely many values. Thus, we get a finite number of Thue equations

$$a_1 \beta_1 \varepsilon_1^n + a_2 \beta_2 \varepsilon_2^n = 1,$$

each of which has only finitely many solutions in $\varepsilon_1, \varepsilon_2$.

Mahler (1933a) proved another generalization of Thue's theorem. Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geq 3$ such that $F(1, 0) \neq 0$ and $F(X, 1)$ has no multiple zeros, and let $p_1, \ldots, p_t$ be distinct primes. Then the equation

$$F(x, y) = \pm p_1^{z_1} \cdots p_t^{z_t}$$

(today called a *Thue–Mahler equation*) has only finitely many solutions in integers $x, y, z_1, \ldots, z_t$ with $\gcd(x, y) = 1$. A consequence of this result, proved by Mahler in a slightly different formulation, is as follows. Let a_1, a_2 be non-zero rational numbers and let Γ be the multiplicative group generated by -1, $p_1, \ldots, p_t$. Then (1) has only finitely many solutions in $x_1, x_2 \in \Gamma$. The argument is similar to that above. By extending the set of primes $p_1, \ldots, p_t$, we may assume that the numerators and denominators of a_1, a_2 are composed of primes from $p_1 \cdots p_t$. Then, by clearing denominators, we can rewrite (1) as

$$u + v = w,$$

where u, v, w are integers, composed of primes from $p_1, \ldots, p_t$, with $\gcd(u, v, w) = 1$. Choose $n \geq 3$. Then we may write u as ax^n and v as by^n, where a, b, x, y are integers composed of primes from $p_1, \ldots, p_t$ and a, b are from a finite set independent of x_1, x_2. Thus, equation (1) can be reduced to a finite number of Thue–Mahler equations as above with $F = aX^n + bY^n$ which all have only finitely many solutions.

Lang (1960) considered equation (1) with unknowns x_1, x_2 taken from a finitely generated multiplicative group, and was the first to realize the central importance of this equation. He proved the general result that if a_1, a_2 are non-zero elements from an arbitrary field K of characteristic 0 and Γ is an arbitrary finitely generated multiplicative subgroup of K^*, then (1) has only finitely many solutions in elements $x_1, x_2 \in \Gamma$. Inspired by Siegel's original result, equations of type (1) with unknowns from a finitely generated multiplicative group are called *unit equations* (in two unknowns), although the group Γ need not be the unit group of a ring. The proofs of all results mentioned above are based on extensions of Thue's method, which are ineffective in the sense that they do not provide a method to determine the solutions of the equations considered above.

In the 1960s, A. Baker developed a new method in transcendence theory, giving non-trivial effective lower bounds for linear forms in logarithms of algebraic numbers. This turned out to be a very powerful tool to prove *effective* finiteness results for Diophantine equations, that enable one to determine all solutions of the equation, at least in principle. With this method, and extensions thereof, it became possible to give explicit upper bounds for the heights of the solutions of Thue equations and Thue–Mahler equations, and also for the

heights of the solutions of equations (1) in units of the ring of integers of a number field or more generally, in *S-units*, these are elements in the number field in whose prime ideal factorizations only prime ideals from a prescribed, finite set S occur. Baker (1968b) obtained explicit upper bounds for the solutions of Thue equations. His result was extended by Coates (1969) to Thue–Mahler equations. For explicit upper bounds for the heights of the solutions of unit equations and S-unit equations in two unknowns, see Győry (1972, 1973, 1974, 1979), and the many subsequent improvements discussed in Chapter 4. The bounds enabled one to determine, at least in principle, all solutions. Since the 1980s, practical algorithms have been developed, combining Baker's theory with the Lenstra–Lenstra–Lovász (LLL) lattice basis reduction algorithm and enumeration techniques, which allow one to solve in practice concrete Thue equations, Thue–Mahler equations and (S-) unit equations, see for instance de Weger (1989), Wildanger (1997) and Smart (1998).

In the 1960s and early 1970s, Schmidt developed his higher dimensional generalization of the Thue–Siegel–Roth method, leading to his *Subspace Theorem* in Schmidt (1972). Schlickewei (1977b) proved an extension of the Subspace Theorem, involving both archimedean and non-archimedean absolute values. Using this so-called p-adic Subspace Theorem, several authors obtained finiteness results for the number of soultions of unit equations in an arbitrary number of unknowns, i.e., for linear equations

$$a_1x_1 + \cdots + a_nx_n = 1 \text{ in } x_1, \ldots, x_n \in \Gamma, \tag{2}$$

where $a_1, \ldots, a_n$ are non-zero elements, and Γ is a finitely generated multiplicative group in a field K of characteristic 0, see Dubois and Rhin (1976), Schlickewei (1977a), Evertse (1984b), Evertse and Győry (1988b) and van der Poorten and Schlickewei (1982, 1991). We mention that the p-adic Subspace Theorem is ineffective, and so its consequences for equation (2) are ineffective. It is still open to solve unit equations of the form (2) in more than two unknowns effectively.

In part I of the book, consisting of the first three chapters, we have collected some basic tools. Chapter 1 gives a collection of the results from elementary algebraic number theory that we need throughout the book. In Chapter 2 we recall some basic facts about algebraic function fields. These are used in Chapters 7 and 8. In Chapter 3 we have stated without proof some fundamental results from Diophantine approximation and transcendence theory. We have included some versions of the Subspace Theorem, due to Schmidt, Schlickewei and Evertse, and estimates of Matveev (2000) and Yu (2007) concerning linear forms in logarithms, which are used in Chapters 4, 5 and 6.

Part II, consisting of the other chapters, is the main body of our book. Chapter 4 provides a survey of effective results concerning unit equations in two unknowns over number fields. We derive among others the best effective upper bounds to date, established in Győry and Yu (2006), for the solutions of equation (1) in S-units of a number field. For applications, we give the bounds in completely explicit form. The main tools in the proofs are the results on linear forms in logarithms mentioned above.

In Chapter 5 we address the problem of practically solving concrete equations of the form (1) in units and S-units. Here, we combine estimates for linear forms in logarithms as mentioned in Chapter 3 with the LLL lattice basis reduction algorithm and an enumeration process.

In Chapter 6, we give an overview of the ineffective theory of unit equations in several unknowns. Among other things, we sketch a proof of the theorem of Evertse, Schlickewei and Schmidt (2002), giving an explicit upper bound for the number of those solutions of (2) for which the left side in (2) has no vanishing subsum. The bound depends only on the number n of unknowns and the rank of Γ. We also include a proof of the theorem of Beukers and Schlickewei (1996) which gives a similar, but sharper, result for equations in two unknowns. Further, we discuss some results giving lower bounds for the number of solutions of unit equations.

In Chapter 7, we deal with analogues over function fields of characteristic 0 of some of the effective and ineffective results discussed in Chapters 4 and 6. In particular, we present the Stothers–Mason abc-theorem due to Stothers (1981) and Mason (1984) for algebraic functions, and a result of Evertse and Zannier (2008) on the number of solutions of unit equations in two unknowns over function fields, analogous to the result of Beukers and Schlickewei mentioned above. Further, we give a brief overview of recent results on unit equations over function fields of positive characteristic.

In Chapter 8, the effective results of Chapters 4 and 7 on S-unit equations in two unknowns over number fields and over function fields are combined with some effective specialization argument to prove a general effective finiteness theorem, due to Evertse and Győry (2013), on the solutions of equation (1) in units x_1, x_2 of an arbitrary, effectively given finitely generated integral domain A over $\mathbb{Z}$.

Chapter 9 deals with applications of unit equations to decomposable form equations, which are higher dimensional generalizations of Thue and Thue–Mahler equations. It is proved that unit equations in an arbitrary number of unknowns are in a certain sense equivalent to decomposable form equations, and in particular unit equations in two unknowns are equivalent to Thue equations. Further, a complete description of the set of solutions of decomposable

form equations is presented. We give explicit upper bounds for the number of solutions when this number is finite. The bounds do not depend on the coefficients of the decomposable forms involved. We also discuss effective results for some important classes of decomposable form equations, including Thue equations, discriminant form equations, and certain norm form equations. The presented results have many applications, especially to algebraic number theory.

The results on unit equations have many further applications to other Diophantine problems. In Chapter 10 we have made a small selection. We give among other things applications to prime factors of sums of integers, additive unit representations in integral domains, dynamics of polynomial maps, arithmetic graphs, irreducible polynomials, equations and inequalities involving discriminants and resultants, power integral bases in number fields, Diophantine geometry, exponential-polynomial equations, and transcendence theory.

As was mentioned in the Preface, a number of applications of the results of the present book are given in our second book *Discriminant Equations in Diophantine Number Theory.*

At the end of several chapters there are Notes in which some historical remarks are made and further related results, generalizations and applications are mentioned.

Contents