

Discriminant Equations in Diophantine Number Theory

Diophantine number theory is an active area that has seen tremendous progress over the past century. An important role in this theory is played by discriminant equations, a class of Diophantine equations with close ties to algebraic number theory, Diophantine approximation and Diophantine geometry. Discriminant equations are about univariate polynomials or binary forms of given discriminant, considered over various types of integral domains.

This book is the first comprehensive account of discriminant equations and their applications. It brings together many aspects, including effective results over number fields, effective results over finitely generated domains, practical algorithms for solving concrete equations, estimates on the number of solutions, applications to algebraic integers of given discriminant, power integral bases, canonical number systems, algorithms for finding a minimal set of generators of an order of a number field, root separation of polynomials and reduction of hyperelliptic curves. The authors' previous title, *Unit Equations in Diophantine Number Theory*, laid the groundwork by presenting important results that are used as tools in the present book. This material is briefly summarized in the introductory chapters along with the necessary basic algebra and algebraic number theory, making the book accessible to experts and young researchers alike.

JAN-HENDRIK EVERTSE is a number theorist, working 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.

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. Győry is also the founder and leader of the Number Theory Research Group in Debrecen, which consists of his former students and their descendants.

NEW MATHEMATICAL MONOGRAPHS

Editorial Board

Béla Bollobás, William Fulton, Anatole Katok, Frances Kirwan, Peter Sarnak,
Barry Simon, Burt Totaro

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.

1. M. Cabanes and M. Enguehard *Representation Theory of Finite Reductive Groups*
2. J. B. Garnett and D. E. Marshall *Harmonic Measure*
3. P. Cohn *Free Ideal Rings and Localization in General Rings*
4. E. Bombieri and W. Gubler *Heights in Diophantine Geometry*
5. Y. J. Ionin and M. S. Shrikhande *Combinatorics of Symmetric Designs*
6. S. Berhanu, P. D. Cordaro and J. Hounie *An Introduction to Involutive Structures*
7. A. Shlapentokh *Hilbert's Tenth Problem*
8. G. Michler *Theory of Finite Simple Groups I*
9. A. Baker and G. Wüstholz *Logarithmic Forms and Diophantine Geometry*
10. P. Kronheimer and T. Mrowka *Monopoles and Three-Manifolds*
11. B. Bekka, P. de la Harpe and A. Valette *Kazhdan's Property (T)*
12. J. Neisendorfer *Algebraic Methods in Unstable Homotopy Theory*
13. M. Grandis *Directed Algebraic Topology*
14. G. Michler *Theory of Finite Simple Groups II*
15. R. Schertz *Complex Multiplication*
16. S. Bloch *Lectures on Algebraic Cycles (2nd Edition)*
17. B. Conrad, O. Gabber and G. Prasad *Pseudo-reductive Groups*
18. T. Downarowicz *Entropy in Dynamical Systems*
19. C. Simpson *Homotopy Theory of Higher Categories*
20. E. Fricain and J. Mashreghi *The Theory of $H(b)$ Spaces I*
21. E. Fricain and J. Mashreghi *The Theory of $H(b)$ Spaces II*
22. J. Goubault-Larrecq *Non-Hausdorff Topology and Domain Theory*
23. J. Śniatycki *Differential Geometry of Singular Spaces and Reduction of Symmetry*
24. E. Riehl *Categorical Homotopy Theory*
25. B. A. Munson and I. Volić *Cubical Homotopy Theory*
26. B. Conrad, O. Gabber and G. Prasad *Pseudo-reductive Groups (2nd Edition)*
27. J. Heinonen, P. Koskela, N. Shanmugalingam and J. T. Tyson *Sobolev Spaces on Metric Measure Spaces*
28. Y.-G. Oh *Symplectic Topology and Floer Homology I*
29. Y.-G. Oh *Symplectic Topology and Floer Homology II*
30. A. Bobrowski *Convergence of One-Parameter Operator Semigroups*
31. K. Costello and O. Gwilliam *Factorization Algebras in Quantum Field Theory I*

Discriminant Equations in Diophantine Number Theory

JAN-HENDRIK EVERTSE
Leiden University, The Netherlands

KÁLMÁN GYŐRY
University of Debrecen, 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/9781107097612

© Jan-Hendrik Evertse and Kálmán Győry 2017

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2017

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

ISBN 978-1-107-09761-2 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Contents

<i>Preface</i>	<i>page xi</i>
<i>Acknowledgments</i>	xii
<i>Summary</i>	xiii
 PART ONE PRELIMINARIES	
1 Finite Étale Algebras over Fields	3
1.1 Terminology for Rings and Algebras	3
1.2 Finite Field Extensions	4
1.3 Basic Facts on Finite Étale Algebras over Fields	6
1.4 Resultants and Discriminants of Polynomials	9
1.5 Characteristic Polynomial, Trace, Norm, Discriminant	11
1.6 Integral Elements and Orders	15
2 Dedekind Domains	17
2.1 Definitions	17
2.2 Ideal Theory of Dedekind Domains	18
2.3 Discrete Valuations	20
2.4 Localization	21
2.5 Integral Closure in Finite Field Extensions	21
2.6 Extensions of Discrete Valuations	22
2.7 Norms of Ideals	24
2.8 Discriminant and Different	25
2.9 Lattices over Dedekind Domains	27
2.10 Discriminants of Lattices of Étale Algebras	30
3 Algebraic Number Fields	34
3.1 Definitions and Basic Results	34
3.1.1 Absolute Norm of an Ideal	34

3.1.2	Discriminant, Class Number, Unit Group and Regulator	35
3.1.3	Explicit Estimates	36
3.2	Absolute Values: Generalities	37
3.3	Absolute Values and Places on Number Fields	39
3.4	S -integers, S -units and S -norm	41
3.5	Heights and Houses	44
3.6	Estimates for Units and S -units	48
3.7	Effective Computations in Number Fields and Étale Algebras	50
3.7.1	Algebraic Number Fields	52
3.7.2	Relative Extensions and Finite Étale Algebras	56
4	Tools from the Theory of Unit Equations	58
4.1	Effective Results over Number Fields	60
4.1.1	Equations in Units of Rings of Integers	60
4.1.2	Equations with Unknowns from a Finitely Generated Multiplicative Group	61
4.2	Effective Results over Finitely Generated Domains	64
4.3	Ineffective Results, Bounds for the Number of Solutions	66
 PART TWO MONIC POLYNOMIALS AND INTEGRAL ELEMENTS OF GIVEN DISCRIMINANT, MONOGENIC ORDERS		
5	Basic Finiteness Theorems	73
5.1	Basic Facts on Finitely Generated Domains	74
5.2	Discriminant Forms and Index Forms	76
5.3	Monogenic Orders, Power Bases, Indices	78
5.4	Finiteness Results	80
5.4.1	Discriminant Equations for Monic Polynomials	80
5.4.2	Discriminant Equations for Integral Elements in Étale Algebras	83
5.4.3	Discriminant Form and Index Form Equations	85
5.4.4	Consequences for Monogenic Orders	86
6	Effective Results over \mathbb{Z}	87
6.1	Discriminant Form and Index Form Equations	89
6.2	Applications to Integers in a Number Field	92
6.3	Proofs	94
6.4	Algebraic Integers of Arbitrary Degree	104

Contents

vii

	6.5 Proofs	106
	6.6 Monic Polynomials of Given Discriminant	108
	6.7 Proofs	109
	6.8 Notes	113
	6.8.1 Some Related Results	113
	6.8.2 Generalizations over \mathbb{Z}	114
	6.8.3 Other Applications	114
7	Algorithmic Resolution of Discriminant Form and Index Form Equations	117
	7.1 Solving Discriminant Form and Index Form Equations via Unit Equations, A General Approach	118
	7.1.1 Quintic Number Fields	121
	7.1.2 Examples	133
	7.2 Solving Discriminant Form and Index Form Equations via Thue Equations	137
	7.2.1 Cubic Number Fields	138
	7.2.2 Quartic Number Fields	138
	7.2.3 Examples	142
	7.3 The Solvability of Index Equations in Various Special Number Fields	145
	7.4 Notes	146
8	Effective Results over the S-integers of a Number Field	148
	8.1 Results over \mathbb{Z}_S	149
	8.2 Monic Polynomials with S -integral Coefficients	152
	8.3 Proofs	157
	8.4 Integral Elements over Rings of S -integers	172
	8.4.1 Integral Elements in Étale Algebras	172
	8.4.2 Integral Elements in Number Fields	178
	8.4.3 Algebraic Integers of Given Degree	179
	8.5 Proofs	182
	8.6 Notes	191
	8.6.1 Historical Remarks	191
	8.6.2 Generalizations and Analogues	192
	8.6.3 The Existence of Relative Power Integral Bases	195
	8.6.4 Other Applications	195
9	The Number of Solutions of Discriminant Equations	196
	9.1 Results over \mathbb{Z}	197
	9.2 Results over the S -integers of a Number Field	200

9.3	Proof of Theorem 9.2.1	202
9.4	Proof of Theorem 9.2.2	205
9.5	Three Times Monogenic Orders over Finitely Generated Domains	209
9.6	Notes	218
10	Effective Results over Finitely Generated Domains	222
10.1	Statements of the Results	223
10.1.1	Results for General Domains	224
10.1.2	A Special Class of Integral Domains	226
10.2	The Main Proposition	228
10.3	Rank Estimates for Unit Groups	229
10.4	Proofs of Theorems 10.1.1 and 10.1.2	231
10.5	Proofs of Theorem 10.1.3 and Corollary 10.1.4	236
10.6	Proofs of the Results from Subsection 10.1.2	239
10.7	Supplement: Effective Computations in Finitely Generated Domains	245
10.7.1	Finitely Generated Fields over \mathbb{Q}	245
10.7.2	Finitely Generated Domains over \mathbb{Z}	249
10.8	Notes	255
11	Further Applications	257
11.1	Number Systems and Power Integral Bases	257
11.1.1	Canonical Number Systems in Algebraic Number Fields	258
11.1.2	Proofs	259
11.1.3	Notes	266
11.2	The Number of Generators of an O_S -order	268
11.2.1	Notes	271
PART THREE BINARY FORMS OF GIVEN DISCRIMINANT		
12	A Brief Overview of the Basic Finiteness Theorems	275
13	Reduction Theory of Binary Forms	278
13.1	Reduction of Binary Forms over \mathbb{Z}	279
13.2	Geometry of Numbers over the S -integers	284
13.3	Estimates for Polynomials	290
13.4	Reduction of Binary Forms over the S -integers	293
14	Effective Results for Binary Forms of Given Discriminant	302
14.1	Results over \mathbb{Z}	303

Contents

ix

14.2	Results over the S -integers of a Number Field	305
14.3	Applications	307
14.4	Proofs of the Results from Section 14.2	311
14.5	Proofs of the Results from Section 14.3	323
14.6	Bounding the Degree of Binary Forms over \mathbb{Z} of Given Discriminant	327
14.7	A Consequence for Monic Polynomials	330
14.8	Relation between Binary Forms of Given Discriminant and Unit Equations in Two Unknowns	332
14.9	Decomposable Forms of Given Semi-Discriminant	333
14.10	Notes	337
14.10.1	Applications to Classical Diophantine Equations	337
14.10.2	Other Applications	338
14.10.3	Practical Algorithms	338
15	Semi-effective Results for Binary Forms of Given Discriminant	339
15.1	Results	340
15.2	The Basic Proposition	342
15.3	Construction of the Tuple	343
15.4	Proof of the Basic Proposition	346
15.5	Notes	356
16	Invariant Orders of Binary Forms	358
16.1	Algebras Associated with a Binary Form	359
16.2	Definition of the Invariant Order	361
16.3	Binary Cubic Forms and Cubic Orders	369
17	On the Number of Equivalence Classes of Binary Forms of Given Discriminant	371
17.1	Results over \mathbb{Z}	372
17.2	Results over the S -integers of a Number Field	374
17.3	Ω -forms	376
17.4	Local-to-Global Results	378
17.5	Lower Bounds	384
17.6	Counting Equivalence Classes over Discrete Valuation Domains	386
17.7	Counting Equivalence Classes over Number Fields	395
17.8	Proofs of the Theorems	401
17.9	Finiteness Results over Finitely Generated Domains	403
17.10	Notes	408

18	Further Applications	409
18.1	Root Separation of Polynomials	409
18.1.1	Results for Polynomials over \mathbb{Z}	410
18.1.2	Results over Number Fields	411
18.1.3	Proof of Theorem 18.1.5	413
18.1.4	Proof of Theorems 18.1.6 and 18.1.7	421
18.1.5	Notes	424
18.2	An Effective Proof of Shafarevich's Conjecture for Hyperelliptic Curves	425
18.2.1	Definitions	426
18.2.2	Results	427
18.2.3	Preliminaries	429
18.2.4	Proofs	430
18.2.5	Notes	435
	<i>Glossary of Frequently Used Notation</i>	436
	<i>References</i>	440
	<i>Index</i>	454