Heights in Diophantine Geometry

The first half of the book is devoted to the general theory of heights and its applications, including a complete, detailed proof of the celebrated subspace theorem of W. M. Schmidt. The second part deals with abelian varieties, the Mordell–Weil theorem and Faltings's proof of the Mordell conjecture, ending wih a self-contained exposition of Nevanlinna theory and the related famous conjectures of Vojta. The book concludes with a comprehensive list of references. It is destined to be a definitive reference book on modern diophantine geometry, bringing a new standard of rigor and elegance to the field.

Professor ENRICO BOMBIERI is a professor of Mathematics at the Institute of Advanced Study, Princeton.

Dr WALTER GUBLER is a lecturer in Mathematics at the University of Dortmund.

New Mathematical Monographs

For information about Cambridge University Press mathematics publications visit http://publishing.cambridge.org/stm/mathematics/

HEIGHTS IN DIOPHANTINE GEOMETRY

Enrico Bombieri
Institute of Advanced Study, Princeton

Walter Gubler
University of Dortmund

CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521846158

First published 2006

Printed in the United Kingdom at the University Press, Cambridge

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

ISBN-13 978-0-521-84615-8 hardback
ISBN-10 0-521-84615-3 hardback

Contents

Cambridge University Press
0521846153 - Heights in Diophantine Geometry
Enrico Bombieri and Walter Gubler
Frontmatter
More information

Preface

Diophantine geometry, the study of equations in integer and rational numbers, is one of the oldest subjects of mathematics and possibly the most popular part of number theory, for the professional mathematician and the amateur alike. Certainly, one of its main attractions is that, far from being a disconnected assembly of isolated results, it provides glimpses of a view which hints at a well-organized underlying structure.

Diophantine equations are of course determined by the underlying algebraic equations and therefore their associated algebraic geometry, obtained by dropping the condition that the solutions must be integers or rational numbers, plays a big role in their study. However, algebraic geometry is already not an easy subject. A pioneer and one of the founding fathers of algebraic geometry, the German mathematician Max Noether, after seeing the theory of algebraic curves with its elegance, simplicity, and also depth of results, and comparing it with the collection of the existing examples of algebraic surfaces at the time, for which nothing comparable could be found, used to say that algebraic curves were created by God and algebraic surfaces by the Devil. Only later, with the development of new tools, in particular the introduction of cohomological and topological methods, the theory of surfaces and higher-dimensional varieties over a field found a satisfactory status.

Of special importance for arithmetic was the development of algebraic geometry over fields of positive characteristic and p-adic fields, since the study of polynomial congruences leads very naturally to such problems. The next big step, the study of varieties over general rings (in contrast to fields), was done by Grothendieck in his monumental construction of the theory of schemes. This provided the basic setting for the study of diophantine equations from a geometric point of view. Bits and pieces of a theory were provided at an early stage (Weil's proof of the Mordell–Weil theorem is possibly the first example) and Weil's theory of heights, with its good arithmetic and geometric properties, was for a long time the main tool. However, the development of a consistent theory was hindered by two major obstacles.

An algebraic curve X over, for example, the ring $\mathbb{Z}$ of rational integers is, from the point of view of schemes, a two-dimensional object, an arithmetic surface, endowed with a morphism $f : X \to \mathrm{Spec}(\mathbb{Z})$. Ideally, we would like to find an analogue of the classical theory of algebraic surfaces which applies in this arithmetic setting.

This can be done only to some extent. First of all, global results require working with complete varieties, and a first problem was to compactify $\mathrm{Spec}(\mathbb{Z})$ and develop a good intersection theory for divisors. This step was brilliantly solved by Arakelov, using adeles and introducing metrics on the "fibre at infinity." Arakelov's work can be regarded as the start of a beautiful new theory, aptly named "arithmetic geometry." As an example, in arithmetic geometry the theory of heights is a special chapter of the much more precise arithmetic intersection theory.

Arakelov's theory did not solve all problems and major questions remain. In the "horizontal direction" given by the base $\mathrm{Spec}(\mathbb{Z})$, infinitesimal methods are no longer at our disposal and genuine new difficulties, with no counterpart in the classical theory, do appear. This is one of the major stumbling blocks for further progress. Thus at the present stage we may take a view half-way towards Max Noether's view: Arithmetic surfaces were also created by God, but their study encounters devilish difficulties.

Today, there are already good books devoted to the subject, and we can mention here Lang's [**169**], Serre's [**277**], the more expository but very comprehensive account of Lang's [**171**] and Hindry and Silverman's [**153**]. So, why a new book on diophantine geometry?

As is often the case, this book grew from introductory lectures at the graduate level, given over a decade ago at the Scuola Normale Superiore di Pisa and the Mathematisches Forschungsinstitut of the Eidgenössische Technische Hochschule in Zürich. An advanced knowledge of algebra or algebraic geometry was not a prerequisite of the courses. Thus the subject was developed mainly through classical lines, namely the theory of varieties over fields of characteristic 0 insofar as algebraic geometry was concerned, and the theory of heights for the number theoretic aspects.

Already with the initial rough notes, embracing the view that in order to learn tools it is best to use them in practice, it was decided to keep mathematical rigor as a strict requirement, supplying references whenever needed and making a clear distinction between a proof and a plausible argument. Examples, including unusual ones, and advanced sections in which deeper aspects of the theory were either developed or described, were included whenever possible. Rather than including this type of material as "exercises" at various levels of difficulty, often disguising good research papers as exercises, it was decided to include proofs and extended comments also for them. However, in the time needed to put the original material together, the subject matter continued to advance at a fast pace, whence the need for inclusion of additional interesting material, as well as substantial revisions of what had been done before.

In the final product, this book is basically divided into three parts. Chapters 1 to 7 develop the elementary theory of heights and its applications to the diophantine geometry of subvarieties of the split torus $\mathbb{G}_m^n$, including applications to diophantine approximation with proofs of Roth's theorem and Schmidt's subspace theorem and some unusual applications.

Chapters 8 to 11 deal with abelian varieties and the diophantine geometry of their subvarieties, ending with a detailed proof of Faltings's celebrated theorem establishing Mordell's conjecture for curves, following Vojta's proof as simplified in [**29**]. However, we felt that a proper treatment of Faltings's big theorem, namely his proof of Lang's conjectures about rational points on subvarieties of abelian varieties, was best done in the context of arithmetic geometry and with regrets we limited ourselves on this matter only to a few comments about the theorem itself and to some of its applications.

Chapters 12 to 14 are more speculative and at times straddle the borderline between diophantine geometry and arithmetic geometry. Chapter 12 deals with the so-called abc-conjecture over number fields, including a complete proof of Belyĭ's theorem and its application to Elkies's theorem, various examples, concluding with a finiteness result for the generalized Fermat equation, due to Darmon and Granville. Chapter 13, which is largely self contained, is an exposition of the classical Nevanlinna theory, with proofs of the first and second main theorems of Nevanlinna, and also Cartan's extension of them to the theory of meromorphic curves. Its purpose is to motivate the final Chapter 14 dealing with the well-known Vojta conjectures, which have spurred a great deal of work in the field.

Proofs are usually given in full detail, but of course it was not feasible to develop all algebra and algebraic geometry from scratch and they tend to be fairly condensed at times. To alleviate this, Appendix A summarizes all concepts of algebraic geometry needed in this book and Appendix B gathers the necessary facts about ramification in number theory and algebraic geometry. Both are provided with complete references to standard books and should help the reader in understanding which notions and notations we use. Finally Appendix C contains an account of Minkowski's geometry of numbers, with proofs, at least to the extent we need in this book.

Some sections in this book appear in small print. Their meaning is simply that they can be omitted in a first reading, either because they require more advanced knowledge of algebra and geometry, or because they deal with side topics not appearing elsewhere in the book. At the end of every chapter, the reader will find some bibliographical notes, containing both historical comments and references to additional literature. However, in no way do these references pretend to be complete and they only represent our personal choices for additional reading.

This book does not represent an introduction to diophantine geometry, nor a complete treatment of the theory of heights. Neither do we strive for maximum generality, and most of the book is concerned only with a number field as ground field, dealing only marginally with the function field case and even less with ground fields of positive characteristic. Also, we do not extend the theory to semiabelian varieties or non-split commutative linear groups, which are also quite important and lead to delicate questions.

The whole theory of effective diophantine approximation, and Baker's theory of logarithmic forms, are missing entirely from this book and relegated to a few comments at the end of Chapter 5. This is not due to a perception of lack of importance of the subject. Rather, an adequate treatment of the topic would have required a second large volume for this already large book.

The same can be said for arithmetic geometry, which no doubt deserves an advanced monograph by itself, also for the arithmetic theory of elliptic curves and abelian varieties, and for the arithmetic theory of modular functions and its applications to diophantine problems.

Our goal in writing this book was to provide, in addition to the existing literature, a wide selection of topics in the subject, containing foundational material with complete proofs, numerous examples, and additional material viewed as a bridge between the classical theory and arithmetic geometry proper. A fair portion of this book is meant to be accessible to a reader with only a basic course in algebra and algebraic geometry, but even the specialist in the field should be able to find interesting material in it. We made no serious attempt to reach completeness about the history of the subject, also referenced material (we never quote from secondary sources) is for this very reason mostly from literature in the English and French languages. Finally, although we attempted to put together a comprehensive bibliography, in no way do we pretend it to be complete. We apologize in advance for the inevitable omissions in our bibliography, regarding priorities and precursor works.

At the end of the book the reader will find an index of mathematical names in lexicographic order and an index of notations ordered by page number. The vanity index (index of authors mentioned in the text) has been omitted.

Terminology

We try to use standard terminology, but for convenience of the reader we gather here some of the most frequently used notation and conventions.

In set theory, $A \subset B$ means that A is a subset of B. In particular, A may be *equal* to B. If this case is excluded, then we write $A \subsetneq B$. The complement of A in B is denoted by $B \setminus A$ as we reserve $-$ for algebraic purposes. We denote the number of elements of A by $|A|$ (possibly ∞). The identity map is id.

A quasi-compact topological space is characterized by the Heine–Borel property for open coverings. In this book, a compact space is quasi-compact *and* Hausdorff.

We denote by $\mathbb{N}$ the set of natural numbers *with* 0 *included* and $\mathbb{Z}$ is the ring of rational integers. Then $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are the fields of rational, real, and complex numbers. A positive number means $x > 0$, but we use $\mathbb{R}_+$ for the non-negative real numbers. The Kronecker symbol δ_{ij} is 0 for $i \neq j$ and 1 for $i = j$.

The real (resp. imaginary) part of a complex number z is denoted by $\Re z$ (resp. $\Im z$) and $\overline{z}$ is complex conjugation.

The floor function $\lfloor x \rfloor$, defined for $x \in \mathbb{R}$, is the largest rational integer $\leq x$. The ceiling function $\lceil x \rceil$ denotes the smallest rational integer $\geq x$.

The real functions on X are denoted by $\mathbb{R}^X$. For $f, g \in \mathbb{R}^X$, the Landau symbol $f = O(g)$ means $|f(x)| \leq Cg(x)$ for some unspecified positive constant C. If we want to emphasize the dependence of C on parameters $\varepsilon, L, \ldots$ we write $f = O_{\varepsilon,L,\ldots}(g)$. As a special case, $f = O(1)$ means that f is a bounded function on X. We also use, with the same meaning, the equivalent Vinogradov's symbol $f \ll g$ and $f \ll_{\varepsilon,L,\ldots} g$. The symbol $g \gg f$ is interpreted as $f \ll g$.

If X is a topological space and f, g are defined on a subset Y with an accumulation point x, then $f = O(g)$ for $y \to x$ means that $|f(y)| \leq Cg(y)$ holds for all $y \in Y$ contained in a neighbourhood of x. If this is true for all $C > 0$ (with neighbourhoods depending on C), then we use the Landau symbol $f = o(g)$ for $y \to x$. The asymptotic relation $f \sim g$ for $y \to x$ means that $f - g = o(|g|)$.

The Landau symbols and the Vinogradov symbol must be used with caution in presence of parameters, not just because the constant involved may depend on parameters, but especially because the neighbourhood in which the inequality holds will also depend on the parameters, an easily overlooked fact.

In number theory, we use $\mathrm{GCD}(a, b)$ for the greatest common multiple of a and b. As usual, $a|b$ means that a divides b. The number of primes up to x is $\pi(x)$.

The group of multiplicative units of a commutative ring with identity is denoted by $R^\times$. We use the symbol V^* to denote the dual of a vector space V. Rings and algebras are always assumed to be associative, fields are always commutative. If the rings have an identity, then we assume that ring homomorphisms send 1 to 1. The ideal generated by $g_1, \ldots, g_m$ is denoted by $[g_1, \ldots, g_m]$. The characteristic of a field K is $\mathrm{char}(K)$ and we write $\mathbb{F}_q$ for the finite field with q elements.

The ring of polynomials in the variable x with coefficients in K is denoted by $K[x]$. A monic polynomial has highest coefficient 1. The minimal polynomial of an algebraic number α over a field is assumed to be monic and its degree is the degree of α, denoted by $\deg(\alpha)$. If we consider the minimal polynomial over $\mathbb{Z}$ (or any factorial ring), then we replace monic by the assumption that the coefficients are coprime. We use $\mathbf{x}$ to denote a vector with entries x_i, thus $K[\mathbf{x}]$ is the ring of polynomials in the variables x_i. By $\overline{K}$ we denote a choice of an algebraic closure of the field K.

For the terminology used in algebraic geometry, the reader is referred to Appendix A.

The numbering in this book is by chapter (appendices in capitals), section, and statement, in progressive order. Equations are numbered separately by chapter (appendices in capitals) and statement in progressive order, with the label enclosed in parentheses. References to equations not occurring on the same page or the preceding page also give the page numbers; the first example is: (A.13) on page 558, occurring on page 15.