Lecture Notes in Mathematics 1566

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

B. Edixhoven J.-H. Evertse (Eds.)

Diophantine Approximation and Abelian Varieties

Springer

Editors

Bas Edixhoven
Institut Mathématique
Université de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex, France

Jan-Hendrik Evertse
Universiteit Leiden
Wiskunde en Informatica
Postbus 9512
NL-2300 RA Leiden, The Netherlands

1st edition 1993
2nd printing 1997 (with minor corrections)
3rd printing 2003

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Diophantine approximation and abelian varieties : introductory lectures / B. Edixhoven ; J.-H. Evertse (ed.). - 2. printing. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hongkong ; London ; Mailand ; Paris ; Santa Clara ; Singapur ; Tokio : Springer, 1997
(Lecture notes in mathematics ; Vol. 1566)
ISBN 3-540-57528-6

Mathematics Subject Classification (1991): 14G05, 14G40, 11J99, 11G35

ISSN 0075-8434
ISBN 3-540-57528-6 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Businiess Media GmbH

Typesetting: Camera-ready TEX output by the author/editor
46/3111-543 - Printed on acid-free paper

Preface

From April 12 to April 16, 1992, the instructional conference for Ph.D-students "Diophantine approximation and abelian varieties" was held in Soesterberg, The Netherlands. The intention of the conference was to give Ph.D-students in number theory and algebraic geometry (but anyone else interested was welcome) some acquaintance with each other's fields. In this conference a proof was presented of Theorem I of G. Faltings's paper "Diophantine approximation on abelian varieties", Ann. Math. 133 (1991), 549–576, together with some background from diophantine approximation and algebraic geometry. These lecture notes consist of modified versions of the lectures given at the conference.

We would like to thank F. Oort and R. Tijdeman for organizing the conference, the speakers for enabling us to publish these notes, C. Faber and W. van der Kallen for help with the typesetting and last but not least the participants for making the conference a successful event.

Contents

Contributors

F. Beukers
Universiteit Utrecht, Mathematisch Instituut, Postbus 80.010, 3508 TA Utrecht, The Netherlands.

B. Edixhoven
Université de Rennes 1, Institut Mathématique, Campus de Beaulieu, 35042 Rennes, France.

J.H. Evertse
Universiteit Leiden, Wiskunde en Informatica, Postbus 9512, 2300 RA Leiden, The Netherlands.

C. Faber
Universiteit van Amsterdam, Wiskunde en Informatica, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands.

G. van der Geer
Universiteit van Amsterdam, Wiskunde en Informatica, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands.

J. Huisman
Université de Rennes 1, Institut Mathématique, Campus de Beaulieu, 35042 Rennes, France.

A.J. de Jong
Princeton University, Fine Hall, Princeton, NJ 08544-0001, U.S.A.

R.J. Kooman
Lijtweg 607, 2341 Oegstgeest, The Netherlands.

F. Oort
Universiteit Utrecht, Mathematisch Instituut, Postbus 80.010, 3508 TA Utrecht, The Netherlands.

M. van der Put
Universiteit Groningen, Wiskunde en Informatica, Postbus 800, 9700 AV Groningen, The Netherlands.

R. Tijdeman
Universiteit Leiden, Wiskunde en Informatica, Postbus 9512, 2300 RA Leiden, The Netherlands.

J. Top
Universiteit Groningen, Wiskunde en Informatica, Postbus 800, 9700 AV Groningen, The Netherlands.

Introduction

Although diophantine approximation and algebraic geometry have different roots, today there is a close interaction between these fields. Originally, diophantine approximation was the branch in number theory in which one deals with problems such as approximation of irrational numbers by rational numbers, transcendence problems such as the transcendence of e or π, etc. There are some very powerful theorems in diophantine approximation with many applications, among others to certain classes of diophantine equations. It turned out that several results from diophantine approximation could be improved or generalized by techniques from algebraic geometry. The results from diophantine approximation which we discuss in detail in these lecture notes are Roth's theorem, which states that for every algebraic number α and for every $\delta > 0$ there are only finitely many $p, q \in \mathbb{Z}$ with $|\alpha - p/q| < |q|^{-2-\delta}$, and a powerful higher dimensional generalization of this, the so-called Subspace theorem of W.M. Schmidt. Here, we would like to mention the following consequence of the Subspace theorem, conjectured by S. Lang and proved by M. Laurent: let Γ be the algebraic group $(\overline{\mathbb{Q}}^*)^n$, endowed with coordinatewise multiplication, V a subvariety of Γ, not containing a translate of a positive dimensional algebraic subgroup of Γ, and G a finitely generated subgroup of Γ; then $V \cap \Gamma$ is finite.

We give a brief overview of the proof of Roth's theorem. Suppose that the equation $|\alpha - p/q| < q^{-2-\delta}$ has infinitely many solutions $p, q \in \mathbb{Z}$ with $q > 0$. First one shows that for sufficiently large m there is a polynomial $P(X_1, \ldots, X_m)$ in $\mathbb{Z}[X_1, \ldots, X_m]$ with "small" coefficients and vanishing with high order at $(\alpha, \ldots, \alpha)$. Then one shows that P cannot vanish with high order at a given rational point $x = (p_1/q_1, \ldots, p_n/q_n)$ satisfying certain conditions. This non-vanishing result, called Roth's Lemma, is the most difficult part of the proof. From the fact that $|\alpha - p/q| < q^{-2-\delta}$ has infinitely many solutions it follows that one can choose x such that $|\alpha - p_n/q_n| < q_n^{-2-\delta}$ for n in $\{1, \ldots, m\}$. Then for some small order partial derivative P_i of P we have $P_i(x) \neq 0$. But $P_i(x)$ is a rational number with denominator dividing $a := q_1^{d_1} \cdots q_m^{d_m}$, where $d_j = \deg_{X_j}(P_i)$. Hence $|P_i(x)| \geq 1/a$. On the other hand, P_i is divisible by a high power of $X_j - \alpha$ and $|p_j/q_j - \alpha|$ is small for all j in $\{1, \ldots, m\}$. Hence $P_i(x)$ must be small. One shows that in fact $|P_i(x)| < 1/a$ and thus one arrives at a contradiction.

Algebraic geometry enables one to study the geometry of the set of solutions (e.g., over an algebraically closed field) of a set of algebraic equations. The geometry often predicts the structure of the set of arithmetic solutions (e.g., over a number field) of these algebraic equations. As an example one can mention Mordell's conjecture, which was proved by G. Faltings in 1983 [21]. Several results of this type have been proved by combining techniques from algebraic geometry with techniques similar to those used in the proof of Roth's theorem. Typical examples are the Siegel-Mahler finiteness theorem for integral points on algebraic curves and P. Vojta's recent proof of Mordell's conjecture.

In these lecture notes, we study the proof of the following theorem of G. Faltings ([22], Thm. I), which is the analogue for abelian varieties of the result for $(\overline{\mathbb{Q}}^*)^n$

mentioned above, and which was conjectured by S. Lang and by A. Weil:

> *Let A be an abelian variety over a number field k and let X be a subvariety of A which, over some algebraic closure of k, does not contain any positive dimensional abelian variety. Then the set of rational points of X is finite.*

(Note that this theorem is a generalization of Mordell's conjecture.) The proof of Faltings is a higher dimensional generalization of Vojta's proof of Mordell's conjecture and has some similarities with the proof of Roth's theorem. Basically it goes as follows. Assume that $X(k)$ is infinite. First of all one fixes a very ample symmetric line bundle $\mathcal{L}$ on A, and norms on $\mathcal{L}$ at the archimedian places of k. Let m be a sufficiently large integer. There exists $x = (x_1, \ldots, x_m)$ in $X^m(k)$ satisfying certain conditions (e.g., the angles between the x_i with respect to the Néron-Tate height associated to $\mathcal{L}$ should be small, the quotient of the height of x_{i+1} by the height of x_i should be big for $1 \leq i < m$ and the height of x_1 should be big). Instead of a polynomial one then constructs a global section f of a certain line bundle $\mathcal{L}(\sigma-\varepsilon, s_1, \ldots, s_m)^d$ on a certain model of X^m over the ring of integers R of k. This line bundle is a tensor product of pullbacks of $\mathcal{L}$ along maps $A^m \to A$ depending on $\sigma-\varepsilon$, the s_i and on d; in particular, it comes with norms at the archimedian places. By construction, f has small order of vanishing at x and has suitably bounded norms at the archimedian places of k. Then one considers the Arakelov degree of the metrized line bundle $x^*\mathcal{L}(\sigma-\varepsilon, s_1, \ldots, s_m)^d$ on $\mathrm{Spec}(R)$; the conditions satisfied by the x_i give an upper bound, whereas the bound on the norm of f at the archimedian places gives a lower bound. It turns out that one can choose the parameters ε, σ, the s_i and d in such a way that the upper bound is smaller than the lower bound.

We mention that the construction of f is quite involved. Intersection theory is used to show that under suitable hypotheses, the line bundles $\mathcal{L}(-\varepsilon, s_1, \ldots, s_m)^d$ are ample on X^m. A new, basic tool here is the so-called Product theorem, a strong generalization by Faltings of Roth's Lemma.

On the other hand, Faltings's proof of Thm. I above is quite elementary when compared to his original proof of Mordell's conjecture. For example, no moduli spaces and no l-adic representations are needed. Also, the proof of Thm. I does not use Arakelov intersection theory. Faltings's proof of Thm. I in [22] seems to use some of it, but that is easily avoided. The Arakelov intersection theory in [22] plays an essential role in the proof of Thm. II of [22], where one needs the notion of height not only for points but for subvarieties; we do not give details of that proof. The only intersection theory that we need concerns intersection numbers obtained by intersecting closed subvarieties of projective varieties with Cartier divisors, so one does not need the construction of Chow rings. The deepest result in intersection theory needed in these notes is Kleiman's theorem stating that the ample cone is the interior of the pseudo-ample cone. Unfortunately, we will have to use the existence and quasi-projectivity of the Néron model over $\mathrm{Spec}(R)$ of A in the proof of Lemma 3.1 of Chapter XI; a proof of that lemma avoiding the use of Néron models would significantly simplify the proof of Thm. I. We believe that for someone with a basic knowledge of algebraic geometry, say Chapters II and III of [27], everything in these notes except for the use of Néron models is not hard to understand. In the case where X is a curve, i.e., Mordell's conjecture, the proof of Thm. I can be considerably simplified; this was done by E. Bombieri in [9].

Let us now describe the contents of the various chapters. Chapter I gives an overview of several results and conjectures in diophantine approximation and arithmetic geometry. After that, the lecture notes can be divided in three parts.

The first of these parts consists of Chapters II–IV; some of the most important results from diophantine approximation are discussed and proofs are sketched of Roth's theorem and of the Subspace theorem.

The second part, which consists of Chapters V–XI, deals with the proof of Thm. I above. Chapters V and VII provide the results needed of the theory of height functions and of intersection theory, respectively. Chapter VIII contains a proof of the Product theorem. This theorem is then used in Chapter IX in order to prove the ampleness of certain $\mathcal{L}(-\varepsilon, s_1, \ldots, s_m)^d$. Chapter X gives a proof of Faltings's version of Siegel's Lemma. Chapter XI finally completes the proof of Thm. I. Chapter VI gives some historical background on how D. Mumford's result on the "widely spacedness" of rational points of a curve of genus at least two over a number field lead to Vojta's proof of Mordell's conjecture.

The third part consists of Chapters XII and XIII. Chapter XII gives an application of Thm. I to the study of points of degree d on curves over number fields. Chapter XIII discusses a generalization by Faltings of Thm. I, which was also conjectured by Lang.

Terminology and Prerequisites

In these notes it will be assumed that the reader is familiar with the basic objects of elementary algebraic number theory, such as the ring of integers of a number field, its localizations and completions at its maximal ideals, and the various embeddings in the field of complex numbers. The same goes more or less for algebraic geometry. To understand the proof of Faltings's Thm. I the reader should be familiar with schemes, morphisms between schemes and cohomology of quasi-coherent sheaves of modules on schemes. In order to encourage the reader, we want to mention that Hartshorne's book [27], especially Chapters II, §§1–8 and III, §§1–5 and §§8–10, contains almost all we need. The two most important exceptions are Kleiman's theorem on the ample and the pseudo-ample cones (see Chapter VII), for which one is referred to [28], and the existence and quasi-projectivity of Néron models of abelian varieties (used in Chapter XI), for which [11] is an excellent reference. At a few places the "GAGA principle" (see [27], Appendix B) and some algebraic topology of complex analytic varieties are used. A less important exception is the theorem of Mordell-Weil, a proof of which can for example be found in Manin's [52], Appendix II, or in [70]; Chapter V of these notes contains the required results on heights on abelian varieties. Almost no knowledge concerning abelian varieties will be assumed. By definition an abelian variety over a field k will be a commutative projective connected algebraic group over k. We will use that the associated complex analytic variety of an abelian variety over $\mathbb{C}$ is a complex torus.

Since these notes are written by various authors, the terminologies used in the various chapters are not completely the same. For example, Chapter I uses a normalization of the absolute values on a number field which is different from the normalization used by the other contributors; the reason for this normalization in Chapter I is clear, since one no longer has to divide by the degree of the number field in question to define the absolute height, but it has the disadvantage that the absolute value no longer just depends on the completion of the number field with respect to the absolute value. Another example is the notion of variety. If k is a field, then by a *(algebraic) variety (defined) over* k one can mean an integral, separated k-scheme of finite type; but one can also mean the following: an *(absolutely irreducible) affine variety (defined) over* k is an irreducible Zariski closed subset in some affine space K^n (K a fixed algebraically closed field containing k) defined by polynomials with coefficients in k, and a *(absolutely irreducible) variety (defined) over* k is an object obtained by glueing affine varieties over k with respect to glueing data given again by polynomials with coefficients in k. As these two notions are (supposed to be) equivalent, no (serious) confusion should arise.