Fundamentals of Diophantine Geometry

Serge Lang

Fundamentals of Diophantine Geometry

Springer-Verlag

Serge Lang
Department of Mathematics
Yale University
New Haven, CT 06520
U.S.A.

AMS Subject Classifications: 10B99, 14GXX

Library of Congress Cataloging in Publication Data
Lang, Serge, 1927–
Fundamentals of diophantine geometry.
1. Diophantine analysis. 2. Geometry, Algebraic.
I. Title.
QA242.L235 1983 512'.74 83-361

An earlier version of this book, *Diophantine Geometry*, was published by Wiley-Interscience.

ISBN 978-1-4419-2818-4 ISBN 978-1-4757-1810-2 (eBook)
DOI 10.1007/978-1-4757-1810-2

Published in 1983 by Springer Science+Business Media New York
Originally published by Springer-Verlag New York Inc in 1983.
Softcover reprint of the hardcover 1st edition 1983

Typeset by Composition House Ltd., Salisbury, England.

9 8 7 6 5 4 3 2 1

Foreword

Diophantine problems represent some of the strongest aesthetic attractions to algebraic geometry. They consist in giving criteria for the existence of solutions of algebraic equations in rings and fields, and eventually for the number of such solutions.

The fundamental ring of interest is the ring of ordinary integers $\mathbf{Z}$, and the fundamental field of interest is the field $\mathbf{Q}$ of rational numbers. One discovers rapidly that to have all the technical freedom needed in handling general problems, one must consider rings and fields of finite type over the integers and rationals. Furthermore, one is led to consider also finite fields, p-adic fields (including the real and complex numbers) as representing a localization of the problems under consideration.

We shall deal with global problems, all of which will be of a qualitative nature. On the one hand we have curves defined over say the rational numbers. If the curve is affine one may ask for its points in $\mathbf{Z}$, and thanks to Siegel, one can classify all curves which have infinitely many integral points. This problem is treated in Chapter VII. One may ask also for those which have infinitely many rational points, and for this, there is only Mordell's conjecture that if the genus is $\geqq 2$, then there is only a finite number of rational points.

On the other hand, we have abelian varieties. If A is an abelian variety defined over $\mathbf{Q}$, then its group of rational points is finitely generated (Mordell–Weil theorem). The proofs do not give a constructive method to get hold of the generators. Abelian varieties include of course curves of genus 1, which have been the fundamental testing ground for conjectures, theorems, and proofs in the theory.

As a curve of genus $\geqq 1$ is characterized by the fact that it is embeddable in an abelian variety, one is led to study subvarieties of abelian varieties, and especially Mordell's conjecture, in this light. A curve of genus $\geqq 2$ is

characterized by the fact that it is unequal to any non-zero translation of itself in its Jacobian. This is a very difficult hypothesis to use.

It is also interesting to look at subvarieties of other group varieties. For us, the natural ones to consider are the toruses, i.e. products of multiplicative groups. It will be shown that if G is such a group, V a curve contained in G, Γ a finitely generated subgroup of G, and $V \cap \Gamma$ is infinite then V is the translation of a subtorus (in characteristic 0).

For various generalizations, and comments on the above results and problems, see Chapters VI and VII and the Historical Notes at the end of these chapters.

The prototypes of the diophantine results and methods given in this book were developed by Mordell, Weil, and Siegel between 1920 and 1930. Considering recent developments in the techniques of algebraic geometry, and Roth's theorem, it seemed quite worth while to give a systematic exposition of the theory as it stands, i.e. essentially a qualitative theory. One of the directions of research at present lies in making theorems quantitative, that is, getting estimates for the number of rational or integral points, or the generators of the Mordell–Weil group. It is a striking feature of the proofs that they are highly non-constructive. There do exist still some unsolved qualitative problems. Aside from Mordell's conjecture, for instance, I would conjecture that Siegel's result on integral points remains true for an affine open subset of an abelian variety, defined over **Z** (or a ring of finite type over **Z**). In general, the extension of Roth's theorem and the theory of integral points as given in Chapter VII to varieties of dimension >1 is still lacking.

New York, 1961 S. LANG

[*The above is reproduced verbatim from* Diophantine Geometry. *Chapters VI and VII are now included in Chapters 7 and 8 respectively.*]

Preface

Diophantine Geometry has been out of print for a while. Advances in algebraic geometry, especially in some of the problems of diophantine geometry, have motivated me to bring out a new book, and I thank Springer-Verlag for publishing it.

Three years after *Diophantine Geometry* appeared, Néron published his fundamental paper giving his canonical heights and explaining how they could be decomposed as sums of local functions. Tate also gave his simple global existence proof for the canonical height. These constitute the main new topics which I treat here. I have also included the Chevalley–Weil theorem; Mumford's theorem concerning heights on curves; Liardet's theorem on the intersection of curves with division points; Schanuel's counting of points in projective space; and theorems of Silverman and Tate on heights in algebraic families.

I still emphasize the Mordell–Weil theorem, Thue–Siegel–Roth theorem, Siegel's theorem on integral points and related results, and the Hilbert irreducibility theorem. These basically depend on heights rather than Néron functions, and so the material on Néron functions (as distinguished from the canonical heights) has been put at the end.

Twenty years ago, the modern period of algebraic geometry was in its infancy. Today the situation is different. Several major advances have not been included although they would be equally worthy. They deserve books to themselves, and I list some of them. Néron's paper proving the existence of a minimal model for abelian varieties was already a book, and only a full new book could do justice to a new exposition of his result and some of its applications; these include Spencer Bloch's interpretation of the Birch–Swinnerton-Dyer conjecture together with its relation to the Néron pairing. I have not included Parsin's and Arakelov's rigidity theorems. I have not

included Manin's proof of the Mordell conjecture over function fields; nor Grauert's subsequent other proof, depending on differential geometric considerations on the curve; nor Parsin's proof of Manin's theorem based on entirely different considerations. I have not included Raynaud's proof that the intersection of a curve with the torsion in an abelian variety is finite, nor Bogomolov's results in this same direction. The methods of proof depend on group schemes and p-adic representations. I have not included Arakelov's intersection theory on arithmetic surfaces. Such results and others would fill several volumes, as a continuation of the present book, which merely lays down the basic concepts of diophantine geometry. And the results mentioned above are some of those with a unity of style relative to the topics chosen here. This leaves out transcendental methods, the theory of equations in many variables (quasi-algebraic closure, circle methods), etc.

When *Diophantine Geometry* first came out in 1961, some people regarded methods of algebraic geometry in number theory as something rather far out, and some mathematicians objected to the general style, as when Mordell wrote (*Bull. AMS* (1964), p. 497): "... When proof of an extension makes it exceedingly difficult to understand the simpler cases, it might sometimes be better if the generalizations were left in the Journals." (Mordell's review and my review of his book are reproduced as an appendix.) Of course, a question here is: "exceedingly difficult" to whom? When?

Mordell wrote that he felt like Rip van Winkle. But great progress in mathematics is often accompanied by such feelings. An algebraic geometer who went to sleep in 1961 and woke up in 1981 also might feel like Rip van Winkle. At the time of the first edition, the foundations of algebraic geometry were about to shift from the van der Waerden–Chevalley–Weil–Zariski methods to the Grothendieck methods. Today we have a more extensive perspective. On the whole, neither will bury the other. They serve different purposes, and even complementary purposes. Just as it is essential to reduce mod p^2 (as in Raynaud's proof), and thereby rely on the full power of schemes and commutative algebra, it is also essential to compute estimates on the coefficients and degrees of algebraic polynomial operations, as in the theory of transcendental numbers and algebraic independence several years ago, and in recent work of Wustholz and others. For these applications, one needs the older coordinates (I was about to write of van der Waerden–Chow–Chevalley–Weil–Zariski) of Lasker, Gordan and the nineteenth century algebraic geometers. Anyone who rejects any part of these contributions does so at their own peril. Furthermore, the fact that estimates of coefficients in algebraic operations occurred during recent times first in the direction of transcendental numbers does not mean that this direction is the only application for them. It is a legitimate, and to many people an interesting point of view, to ask that the theorems of algebraic geometry from the Hilbert Nullstellensatz to the most advanced results should carry with them estimates on the coefficients occurring in these theorems. Although some of the estimates are routine, serious and interesting problems arise in this context.

As in *Diophantine Geometry* the content of the present volume is still essentially qualitative. My conjecture that there is only a finite number of integral points on an affine open subset of an abelian variety is still unproved. Roth's theorem is still not effective, and the main advance has been due to Schmidt's generalizations to higher dimensions.

My introduction to *Elliptic Curves*: *Diophantine Analysis* makes it unnecessary to discuss here once more the relative roles of general theorems and concrete examples or special cases, which are complementary. The present book is addressed to those whose taste lies with abelian varieties.

New Haven, 1983 S. LANG

As this book goes to press, Faltings has announced his proof of the Mordell conjecture.

Arbeitstagung, Bonn
June 1983

Contents

Acknowledgment

I thank Michel Laurent and Michel Waldschmidt for useful comments. I am especially indebted to Joe Silverman for his thorough going over of the manuscript and a long list of valuable suggestions and corrections. I am also indebted to Silverman and Tate for their manuscripts which formed the basis for the next to last chapter.

Some Standard Notation

The following notation is used in a standard way throughout.

Rings are assumed commutative and without divisors of 0, unless otherwise specified.

$\boldsymbol{\mu}$	group of all roots of unity.
$\boldsymbol{\mu}(K)$	subgroup of roots of unity in a field K.
R^*, K^*	invertible elements in a ring R (resp. in a field K).
K^a	algebraic closure of a field K.
$K(P)$	field obtained by adjoining to K a set of affine coordinates for a point P (equal to $K(x_0/x_i, \ldots, x_n/x_i)$ if $(x_0, \ldots, x_n)$ are projective coordinates for P).
$R(\mathfrak{a})$	$R/\mathfrak{a}$ for any ideal $\mathfrak{a}$.
$\mathbf{Z}(N)$	$\mathbf{Z}/N\mathbf{Z}$.
$A^{(p)}$	p-primary part of an abelian group A (that is, the subgroup of elements whose order is a power of p).
A_m	subgroup of elements x in an abelian group A such that $mx = 0$.
$[n]$	multiplication by an integer n on an abelian group.
$V(K)$	set of K-valued points of a variety or scheme V.
$D \sim D'$	for divisors D, D', linear equivalence.
$D \approx D'$	for divisors D, D', algebraic equivalence.
$\mathrm{Div}(V)$	group of divisors on a variety V.
$\mathrm{Div}_a(V)$	subgroup of divisors algebraically equivalent to 0.
$\mathrm{Div}_l(V)$	subgroup of divisors linearly equivalent to 0.

$\mathrm{Pic}(V)$	$\mathrm{Div}(V)/\mathrm{Div}_l(V)$.
$\mathrm{Pic}_0(V)$	$\mathrm{Div}_a(V)/\mathrm{Div}_l(V)$.
$\mathrm{NS}(V)$	$\mathrm{Div}(V)/\mathrm{Div}_a(V)$ (the **Néron–Severi** group of V).
$h \sim h'$	equivalence for functions, $\lvert h - h' \rvert$ is bounded.
$h \approx h'$	quasi-equivalence for functions: for each $\varepsilon > 0$, $$-C_1 + (1 - \varepsilon)h \leqq h' \leqq (1 + \varepsilon)h + C_2.$$
$h \ll h'$	for functions, with h' positive, there exists a constant $C > 0$ such that $\lvert h \rvert \leqq Ch'$. Same as $h = O(h')$.
$h \gg\ll h'$	both h, h' positive, $h \ll h'$ and $h' \ll h$.

Usually h, H denote **heights** with $h = \log H$. These are indexed to specify qualifications:

h_φ	height determined by a morphism φ into projective space.
k_K	height relative to a field K.
h_X	height determined by a morphism derived from the linear system $\mathscr{L}(X)$, well defined up to $O(1)$.
h_c	on an arbitrary variety, the height associated with a divisor class c, determined only up to $O(1)$; on an abelian variety, the canonical height.
$\hat{h}_c$	canonical height if one needs to distinguish it from an equivalence class of heights.

Standard references:

IAG = *Introduction to Algebraic Geometry* [L 2].

AV = *Abelian Varieties* [L 3].

Weil's *Foundations* is still quoted in canonical style, F^2–X_y, Theorem Z, which refers to the second edition.

For schemes, see Hartshorne's *Algebraic Geometry*, and also Mumford's *Abelian Varieties.*