# Encyclopaedia of Mathematical Sciences

Volume 60

Editor-in-Chief: R.V. Gamkrelidze

## BOOKS OF RELATED INTEREST BY SERGE LANG

***Fundamentals of Diophantine Geometry***

A systematic account of fundamentals, including the basic theory of heights, Roth and Siegel's theorems, the Néron–Tate quadratic form, the Mordell–Weil theorem, Weil and Néron functions, and the canonical form on a curve as it related to the Jacobian via the theta function.

***Introduction to Complex Hyperbolic Spaces***

Since its introduction by Kobayashi, the theory of complex hyperbolic spaces has progressed considerably. This book gives an account of some of the most important results, such as Brody's theorem, hyperbolic imbeddings, curvature properties, and some Nevanlinna theory. It also includes Cartan's proof for the Second Main Theorem, which was elegant and short.

***Elliptic Curves: Diophantine Analysis***

This systematic account of the basic diophantine theory on elliptic curves starts with the classical Weierstrass parametrization, complemented by the basic theory of Néron functions, and goes on to the formal group, heights and the Mordell–Weil theorem, and bounds for integral points. A second part gives an extensive account of Baker's method in diophantine approximation and diophantine inequalities which were applied to get the bounds for the integral points in the first part.

## OTHER BOOKS BY LANG PUBLISHED BY SPRINGER-VERLAG

Introduction to Arakelov Theory • Riemann–Roch Algebra (with William Fulton) • Complex Multiplication • Introduction to Modular Forms • Modular Units (with Daniel Kubert) • Introduction to Algebraic and Abelian Functions • Cyclotomic Fields I and II • Elliptic Functions • Algebraic Number Theory • $SL_2(R)$ • Abelian Varieties • Differential Manifolds • Complex Analysis • Undergraduate Analysis • Undergraduate Algebra • Linear Algebra • Introduction to Linear Algebra • Calculus of Several Variables • First Course in Calculus • Basic Mathematics • Geometry: A High School Course (with Gene Murrow) • Math! Encounters with High School Students • The Beauty of Doing Mathematics • THE FILE

Serge Lang (Ed.)

# Number Theory III

## Diophantine Geometry

Springer-Verlag Berlin Heidelberg GmbH

Title of the Russian edition:
Itogi nauki i tekhniki, Sovremennye problemy matematiki,
Fundamental'nye napravleniya.
Vol. 60, Teoriya Chisel 3
Publisher VINITI, Moscow.

Mathematics Subject Classification (1980): 11Dxx, 11Gxx,
14Dxx, 14Gxx, 14Hxx, 14Kxx

Library of Congress Cataloging-in-Publication Data
Number theory III : diophantine geometry / Serge Lang (ed.).
p. cm. — (Encyclopaedia of mathematical sciences : v. 60)
Includes bibliographical references and index.
ISBN 978-3-540-61223-0 ISBN 978-3-642-58227-1 (eBook)
DOI 10.1007/978-3-642-58227-1
1. Diophantine analysis. I. Lang, Serge, 1927– II. Title:
Number theory 3. III. Title: Diophantine geometry. IV. Series.
QA242.N85 1991
512'.7—dc20 91-17718
CIP



Originally published by Springer-Verlag Berlin Heidelberg New York in 1991
Softcover reprint of the hardcover 1st edition 1991

Typesetting: Asco Trade Typesetting Ltd., Hong Kong
2141/3140-543210—Printed on acid-free paper

# List of Editors and Contributors

*Editor-in-Chief*

R. V. Gamkrelidze, Academy of Sciences of the USSR, Steklov Mathematical Institute, ul. Vavilova 42, 117966 Moscow, Institute for Scientific Information (VINITI), Usievich ul. 20, 125219 Moscow, USSR

*Consulting Editor and Author*

S. Lang, Department of Mathematics, Yale University, New Haven, CT 06520, USA

# Preface

In 1988 Shafarevich asked me to write a volume for the Encyclopaedia of Mathematical Sciences on Diophantine Geometry. I said yes, and here is the volume.

By definition, diophantine problems concern the solutions of equations in integers, or rational numbers, or various generalizations, such as finitely generated rings over $\mathbf{Z}$ or finitely generated fields over $\mathbf{Q}$. The word Geometry is tacked on to suggest geometric methods. This means that the present volume is not elementary. For a survey of some basic problems with a much more elementary approach, see [La 90c].

The field of diophantine geometry is now moving quite rapidly. Outstanding conjectures ranging from decades back are being proved. I have tried to give the book some sort of coherence and permanence by emphasizing structural conjectures as much as results, so that one has a clear picture of the field. On the whole, I omit proofs, according to the boundary conditions of the encyclopedia. On some occasions I do give some ideas for the proofs when these are especially important. In any case, a lengthy bibliography refers to papers and books where proofs may be found. I have also followed Shafarevich's suggestion to give examples, and I have especially chosen these examples which show how some classical problems do or do not get solved by contemporary insights. Fermat's last theorem occupies an intermediate position. Although it is not proved, it is not an isolated problem any more. It fits in two main approaches to certain diophantine questions, which will be found in Chapter II from the point of view of diophantine inequalities, and Chapter V from the point of view of modular curves and the Taniyama–Shimura conjecture. Some people might even see a race between the two approaches: which one will prove Fermat first? It

is actually conceivable that diophantine inequalities might prove the Taniyama–Shimura conjecture, which would give a high to everybody. There are also two approaches to Mordell's conjecture that a curve of genus $\geqq 2$ over the rationals (or over a number field) has only a finite number of rational points: via $l$-adic representations in Chapter IV, and via diophantine approximations in Chapter IX. But in this case, Mordell's conjecture is now Faltings' theorem.

Parts of the subject are more accessible than others because they require less knowledge for their understanding. To increase accessibility of some parts, I have reproduced some definitions from basic algebraic geometry. This is especially true of the first chapter, dealing with qualitative questions. If substantially more knowledge was required for some results, then I did not try to reproduce such definitions, but I just used whatever language was necessary. Obviously decisions as to where to stop in the backward tree of definitions depend on personal judgments, influenced by several people who have commented on the manuscript before publication.

The question also arose where to stop in the direction of diophantine approximations. I decided not to include results of the last few years centering around the explicit Hilbert Nullstellensatz, notably by Brownawell, and related bounds for the degrees of polynomials vanishing on certain subsets of group varieties, as developed by those who needed such estimates in the theory of transcendental numbers. My not including these results does not imply that I regard them as less important than some results I have included. It simply means that at the moment, I feel they would fit more appropriately in a volume devoted to diophantine approximations or computational algebraic geometry.

I have included several connections of diophantine geometry with other parts of mathematics, such as PDE and Laplacians, complex analysis, and differential geometry. A grand unification is going on, with multiple connections between these fields.

*New Haven* Serge Lang
*Summer* 1990

**Acknowledgment**

I want to thank the numerous people who have made suggestions and corrections when I circulated the manuscript in draft, especially Chai, Coleman, Colliot-Thélène, Gross, Parshin and Vojta. I also thank Chai and Colliot-Thélène for their help with the proofreading.

S.L.

# Contents

# Notation

Some symbols will be used throughout systematically, and have a more or less universal meaning. I list a few of these.

$F^a$ denotes the algebraic closure of a field $F$. I am trying to replace the older notation $\bar{F}$, since the bar is used for reduction mod a prime, for complex conjugates, and whatnot. Also the notation $F^a$ is in line with $F^s$ or $F^{nr}$ for the separable closure, or the unramified closure, etc.

$\#$ denotes number of elements, so $\#(S)$ denotes the number of elements of a set $S$.

$\ll$ is used synonymously with the big Oh notation. If $f$, $g$ are two real functions with $g$ positive, then $f \ll g$ means that $f(x) = O(g(x))$. Then $f \gg\ll g$ means $f \ll g$ and $g \ll f$.

$A[\varphi]$ means the kernel of a homomorphism $\varphi$ when $A$ is an abelian group.

$A[m]$ is the kernel of multiplication by an integer $m$.

*Line sheaf* is what is sometimes called an invertible sheaf. The French have been using the expression "faisceau en droites" for quite some time, and there is no reason to lag behind in English.

*Vector sheaf* will, I hope, replace locally free sheaf of finite rank, both because it is shorter, and because the terminology becomes functorial with respect to the ideas. Also I object to using the same expression vector bundle for the bundle *and* for its sheaf of sections. I am fighting an uphill battle on this, but again the French have been using faisceau vectoriel, so why not use the expression in English, functorially with respect to linguistics?