Grundlehren der mathematischen Wissenschaften 231

A Series of Comprehensive Studies in Mathematics

Serge Lang

Elliptic Curves Diophantine Analysis

Springer-Verlag Berlin Heidelberg GmbH 1978

Serge Lang

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

AMS Subject Classification (1970): 10 B 45, 10 F 99, 14 G 25, 14 H 25

ISBN 978-3-642-05717-5 ISBN 978-3-662-07010-9 (eBook)
DOI 10.1007/978-3-662-07010-9

Library of Congress Cataloging in Publication Data. Lang, Serge, 1927–. Elliptic curves (Grundlehren der mathematischen Wissenschaften: 231). Bibliography: p. Includes index. 1. Diophantine analysis. 2. Curves, Elliptic. I. Title. II. Series: Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen; 231. QA242.L234. 512'.74. 77–21139.

Originally published by Springer-Verlag Berlin Heidelberg New York in 1978

Typesetting: William Clowes & Sons Limited, London, Beccles and Colchester.

2141/3140–543210

Foreword

It is possible to write endlessly on elliptic curves. (This is not a threat.) We deal here with diophantine problems, and we lay the foundations, especially for the theory of integral points. We review briefly the analytic theory of the Weierstrass function, and then deal with the arithmetic aspects of the addition formula, over complete fields and over number fields, giving rise to the theory of the height and its quadraticity. We apply this to integral points, covering the inequalities of diophantine approximation both on the multiplicative group and on the elliptic curve directly. Thus the book splits naturally in two parts.

The first part deals with the ordinary arithmetic of the elliptic curve: The transcendental parametrization, the p-adic parametrization, points of finite order and the group of rational points, and the reduction of certain diophantine problems by the theory of heights to diophantine inequalities involving logarithms. The second part deals with the proofs of selected inequalities, at least strong enough to obtain the finiteness of integral points.

The historical development is such that the first part represents a relatively mature state of the subject, whereas the second part is in a state of flux (due in large measure to the Baker method), so that no current account can be regarded as in any way definitive. The selection of which theorems and which methods to include was based on emphasizing the analogy between operations on the multiplicative group and operations on the elliptic curve, and was meant to give typical results, for instance the first inequality of Baker–Feldman, whose proof is less involved than some others, and is similar to the proof in the subsequent chapter working directly with the elliptic logarithms. The last two chapters illustrate two methods of descent (due to Baker, with some improvements from Cijsouw–Waldschmidt, Tijdeman and Van der Poorten). At the moment they have no analogue in the elliptic case, but it seemed important to make available to the reader as many methods as possible. Finally, the theorem given there (Baker–Tijdeman) leads to the Catalan problem, and it would be interesting to have analogous formulations for elliptic curves.

Elliptic curves serve as a prototype for abelian varieties, as a special case of curves, and as a means of handling other curves by the theory of correspondences. Using concrete formulas, one can get into the theory of elliptic curves without much mathematical background, and one can reach rapidly substantial levels of depth.

However, it should not be forgotten that curves of higher genus ultimately require a thorough understanding of their Jacobians, which cannot avoid the tools developed by algebraic geometers in the last 30 years. Mazur's success in proving that some simple factor of the Jacobian of modular curves over the rationals has

only a finite number of rational points is a testimony to the power of the most general tools provided by algebraic geometry. Via this higher dimensional theorem, one obtains bounds for torsion points on elliptic curves over the rationals which so far have not been obtained by other methods. Thus even as the elliptic curves affect the diophantine properties of other curves, conversely curves of higher genus like the modular curves, or the Fermat curve as in Demyanenko or Kubert-Lang affect the diophantine properties of elliptic curves.

Parallel to the pure arithmetic theory over number fields lies the algebraic-geometric theory of algebraic systems (over the complex numbers if you wish), where sections play the role of rational points. This is the point of view taken in *Diophantine Geometry*. Its origin lay in Severi's recognition of the connection between the "theorem of the base" (finite generation of the group of divisor classes modulo algebraic equivalence) and the Mordell–Weil theorem (finite generation of the group of rational points on an abelian variety). The theorem of the base was proved by Néron in his thesis, and a closer tie between the two theorems was established by Lang–Néron, formulating the relative Mordell–Weil theorem for algebraic families of abelian varieties (the group of sections modulo constant sections is finitely generated). In dimension 1, I showed how the presence of infinitely many integral sections in a family of affine curves of genus $\geqq 1$ implies that the family splits, and almost all sections come from constant ones. My conjecture (transposing Mordell's) that for genus $\geqq 2$ this should also apply to rational sections was proved by Manin. Another proof was subsequently given by Grauert. Both proofs lead, in different ways, to differential geometric considerations on the fiber space. Shafarevič's theorem that there is only a finite number of elliptic curves (up to isomorphism) over a number field, having good reduction outside a given finite set of primes led to Paršin's results along these lines for algebraic families of curves. Néron's classification of minimal models of elliptic curves over discrete valuation rings parallels Kodaira's classification of pencils of elliptic curves. All of these results would make up a nice new volume of diophantine geometry. (Incidentally, Seligman has observed that the Néron–Kodaira diagrams are dual to the Dynkin diagrams in the theory of Lie algebras. No theoretical reason for this has yet been found.)

The methods used for the problems just mentioned have an essentially algebraic aspect. It is also possible to transport the problems to a setting involving the geometry of several complex variables. Curves of genus $\geqq 2$ may be viewed as the 1-dimensional versions of quotients of bounded domains, or of varieties of "general type". I formulated some analogues of the classical diophantine problems in this context, and some of these have been proved recently, e.g. by Kobayashi and Ochai, the finiteness of the number of surjective meromorphic maps onto varieties of general type; and Mark Green, the hyperbolicity of a subvariety of an abelian variety which does not contain the translation of an abelian subvariety. Conjectures as in [L 5] lead to conjectures concerning algebraic families of abelian varieties, or elliptic curves, over the complex numbers. Assuming for simplicity that the family has no fixed part, let $\sigma_1, \ldots, \sigma_r$ be meromorphic sections, linearly independent over the integers. In each fiber we have a metric corresponding to the torus, and one can define a norm on sections as the sup norm over all points of the parameter variety, in

a fixed small neighborhood U of a point. Then the complex analytic analogue of the Baker–Feldman theorem should be that a linear combination of sections satisfies an inequality

$$\|q_1\sigma_1 + \cdots + q_r\sigma_r\|_U \geqq q^{-C},$$

where $q = \max |q_i|$, and C is some constant.

Even as diophantine questions from number theory give rise to problems in geometry (algebraic and differential), conversely number theory can also profit from the techniques of several complex variables (e.g. as introduced by Bombieri–Lang in the theory of transcendental numbers and diophantine approximation, and pursued by Masser, with his theorem asserting that a polynomial having sufficiently many zeros in the unit ball, not too far apart as a function of the degree, must in fact be identically zero).

An advanced monograph like *Diophantine Geometry*, presupposing substantial knowledge in some fields, and thus allowing certain expositions at a level which may be appreciated only by a few, but achieving a certain coherence not otherwise possible, of course does not preclude the writing of elementary monographs. Both coexist amicably. Each achieves different ends. In some sense the present book corresponds to *Diophantine Geometry* on elliptic curves, although of course the theory goes further in the light of progress made in the last 15 years. This is entirely consistent with my conclusion of the review of the first portion of Grothendieck's *Éléments de Géometrie Algébrique* (*Bulletin* AMS, 1961):

> "...If Algebraic Geometry really consists of (at least) 13 chapters, 2,000 pages, all of commutative algebra, then why not just give up? [I was optimistic, it's more like 7,000 pages by now...]
>
> The answer is obvious. On the one hand, to deal with special topics which may be of particular interest only portions of the whole work are necessary, and shortcuts can be taken to arrive faster at specific goals...Projective methods, which have for some geometers a particular attraction of their own, and which are of primary importance in some aspects of geometry, for instance the theory of heights, are of necessity relegated to the background in the local viewpoint of *Elements*, but again may be taken as starting point given a prejudicial approach to certain questions.
>
> But even more important, theorems and conjectures still get discovered and tested on special examples, for instance elliptic curves or cubic forms over the rational numbers. And to handle these, the mathematician needs no great machinery, just elbow grease and imagination to uncover their secrets. Thus as in the past, there is enough stuff lying around to fit everyone's taste. Those whose taste allows them to swallow the *Elements*, however, will be richly rewarded."

On the other hand, the present book is addressed to those whose taste lies with elliptic curves.

Serge Lang

Acknowledgment

I am much indebted to Michel Waldschmidt, Neal Koblitz and David Rohrlich for reading through the manuscript carefully, and for a large number of very useful comments.

I thank Addison Wesley for letting me reprint the first few sections in Chapter I from *Elliptic Functions*, concerning the standard properties of the Weierstrass functions.

I thank the editors of Springer-Verlag for their willingness to share with me the excitement which seems to accompany occasionally the publication of my books. They deserved my acquiescence to their request to eliminate from the foreword statements (not necessarily by me) which might be interpreted as perpetuating unnecessary polemics.

Table of Contents