Introduction

The name "diophantine" comes from the ancient mathematician Diophantus of Alexandria (about 250 CE), who wrote a treatise on mathematical problems in which solutions in integer or rational numbers were required.[1] So an equation is *diophantine* when we seek solutions in integers or rationals. Naturally, the word "seek" is not mathematically well defined: by this we are thinking of problems such as

(i) establish whether a given equation has solutions or not, or

(ii) find all solutions, or

(iii) describe, in some simple way, the distribution of solutions, if there are infinitely many.

Depending on the case, we shall meet all of these viewpoints, but, needless to say, only in rather special cases; actually, it has already been proved by Matjiasevic in 1970 that question (i) does not admit a complete algorithmic solution (a negative answer to Hilbert problem X). Also, the general level of these lectures has to be considered introductory, elementary, and self-contained.

Throughout, we shall often adopt a geometrical language, viewing the solutions of an equation (or system of equations) as points in a cartesian space, defining a *variety*. The points with integer (or rational) coordinates will be called integer (or rational) points. In this view, and because a rational number is defined by a *ratio* rather than a *pair* of integers, the distinction between integer and rational solutions roughly corresponds to considering varieties in affine and projective spaces.

We shall focus mainly on *affine* diophantine problems, and moreover on the special case of curves, in practice seeking integer solutions of equations in two variables. This case historically suggested some major ideas for more general problems. We shall present the important connections with diophantine approximation, and prove Thue's celebrated results. However, we shall not provide details for subsequent deeper and more refined investigations, in order to better stress the main principles. In later chapters we shall also treat some (more modern) diophantine problems in a generalized sense, that is, with algebraic points, not restricted to $\mathbb{Q}$ or a number field, and subject to new restrictions (for instance, having small height). The corresponding results, although apparently far from the "classical" ones, will be shown to have relevant applications to ordinary diophantine equations as well.

More precisely, here is a description of the contents of the whole volume:

In Chapter 1 we shall recall the easy cases of equations in one variable and the linear case of two variables; then we shall give the general theory of quadratic

[1] This consisted of several books, of which only a part has survived to our times.

equations in integers, which boils down to the Pell equation. We shall point out the link between these problems and diophantine approximation.

Chapter 2 will be mainly concerned with Thue's theorems for diophantine equations $f(X, Y) = c$, with homogeneous f. We shall present the relation between this and rational approximations to algebraic numbers, and we shall prove Thue's diophantine approximation theorem in full detail. As a corollary, his finiteness theorem for equations will follow. We shall recall without proof some sharpenings that occurred in diophantine approximation after Thue, notably the Roth theorem; we have preferred to give the proof of Thue's theorem only, because it contains many of the basic principles, whereas the proofs of more refined results tend to become rather complicated in detail, with the risk of obscuring some ideas from the beginner. Preliminary to the proofs, we shall explain the main steps of the underlying strategy. As in Chapter 1, we shall stick to "classical" integer solutions, namely over $\mathbb{Z}$.

In Chapter 3 we shall start to formulate diophantine problems over number fields. We shall introduce the fundamental concept of (Weil) *height* and develop in detail some of its main properties. Then we shall formulate without proof the general Roth theorem in diophantine approximation, and present some applications of it, to the Thue–Mahler equation and to the S-unit equation. Finally, also for later use, we shall study the height on finitely generated multiplicative groups of algebraic numbers, interpreting it as a norm on a euclidean space.

In Chapter 4 we shall discuss a kind of diophantine problem in which the variables are free to run over $\overline{\mathbb{Q}}$, but are subject to other arithmetical restrictions; an instance is provided by solutions of equations in roots of unity of arbitrarily high order; in geometrical language, this corresponds to the search for torsion points on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$. We shall explore the more general problem of algebraic points with "small" height, which represents the toric case of a conjecture by F. Bogomolov. This was solved by S. Zhang around 1995, with rather sophisticated methods from Arakelov theory. We shall present an elementary proof of Zhang's theorem, and develop some consequences. We shall also sketch an independent elementary approach by Y. Bilu, relying on his equidistribution theorem for Galois conjugates of algebraic numbers with small height.

In Chapter 5 we shall go back to the S-unit equation and S-unit theorem, already discussed in Chapter 3. This theorem is important for several reasons; in particular, it implies a finiteness theorem for Thue–Mahler equations, as shown in Chapter 3. In that chapter the S-unit theorem is deduced from the general Roth theorem, not proved in these notes. To fill this gap, a complete independent proof of the S-unit theorem will now be given. This proof (by Beukers and Schlickewei) is quantitative and yields a very sharp estimate for the number of solutions. As a corollary, we shall obtain a quantitative estimate for the number of solutions of the Thue–Mahler equation. Some fundamental ingredients for the uniformity of these estimates come from Chapter 4.

The first four chapters are concluded with some "supplements", consisting of various material related to the topics of the chapter.

The "Supplements to Chapter 1" concern two applications of the Dirichlet lemma in diophantine approximation, a solution of the Pell equation $x^2 - py^2 = -1$ (p a prime $\equiv 1 \pmod 4$) expressed in terms of p-th roots of unity, a Pell equation in polynomials, a proof of the irrationality of e^n and of π, an algorithm for rational points on conics, and Fermat's theorem on the nonexistence of right-angled triangles with rational sides and square area. All of these topics are treated in a self-contained way.

The "Supplements to Chapter 2" assume a little more knowledge from the geometry of algebraic curves. Siegel's finiteness theorem for integral points is stated without proof. However, certain interesting cases (like the "double Pell equation" and a case of S-unit equation) are dealt with (over $\mathbb{Z}$) by means only of Thue's theorem. The remaining supplements consist of an algorithm to test the existence of infinitely many integral points on a rational curve, Runge's theorem on integral points and a very brief discussion of a version of Thue's equation for polynomials.

The "Supplements to Chapter 3" contain a full treatment of the S-unit equation over function fields, proving the so-called Mason–Stothers abc-theorem; an alternative approach with respect to known proofs also appears, which leads to similar conclusions for curves more general than $X + Y = 1$. Then, as applications of the elementary theory of heights, we have included an algorithm to compute the multiplicative dependence relations among given algebraic numbers, and a specialization theorem for multiplicative dependence of rational functions on curves and their values; this last issue has been the object of much recent work by several authors.

Finally, the "Supplements to Chapter 4" contain the basic theory of closed subgroups of $\mathbb{R}^n$ (with an application to Kronecker's theorem in simultaneous diophantine approximation) and the Skolem–Mahler–Lech theorem on the zeros of recurrences, together with a significant rephrasing and generalization of the context of algebraic groups. (An "open question" is also stated for sequences arising from Taylor expansions of algebraic functions.)

The book is concluded with an appendix by F. Amoroso, dealing with the problems of Chapter 4 from a quantitative viewpoint. This direction has been the object of much recent research. The appendix mentions several recent results, and a few sketches of some methods of proof.