

## Rational points on curves

Henri Darmon

ABSTRACT. This article surveys a few of the highlights in the arithmetic of curves: the proof of the Mordell Conjecture, and the more detailed theory that has developed around the classes of curves most studied until now by number theorists: modular curves, Fermat curves, and elliptic curves.

### CONTENTS

Introduction	7
1. Preliminaries	13
2. Faltings' theorem	16
3. Modular curves and Mazur's theorem	25
4. Fermat curves	35
5. Elliptic curves	42
References	51

### Introduction

Algebraic number theory is first and foremost the study of Diophantine equations. Such a definition is arguably too narrow for a subject whose scope has expanded over the years to encompass an ever-growing list of fundamental notions: number fields and their class groups, abelian varieties, moduli spaces, Galois representations,  $p$ -divisible groups, modular forms, Shimura varieties, and  $L$ -functions, to name just a few. All of these subjects will be broached (sometimes too briefly, for reasons having less to do with their relative importance than with limitations of time, space, and the author's grasp of the subject) in this survey, which is devoted to the first nontrivial class of Diophantine equations: those associated to varieties of dimension one, or *algebraic curves*.

The term *Diophantine equation* refers to a system of polynomial equations

---

2000 *Mathematics Subject Classification*. Primary 11G30, Secondary 11G05, 11G18, 11G40, 14G05, 14G35.

$$(1) \quad X : \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \quad (\text{with } f_i \in \mathbf{Z}[x_1, \dots, x_n]).$$

Given such a system, one wishes to understand (and, if possible, determine completely) its set of integer or rational solutions.

Little of the essential features of the question are lost, and much flexibility is gained, if one replaces the base ring  $\mathbf{Z}$  by a more general ring  $\mathcal{O}$ . The prototypical examples are the ring of integers  $\mathcal{O}_K$  of a number field  $K$ , or the ring  $\mathcal{O}_{K,S}$  of its  $S$ -integers, for a suitable finite set  $S$  of primes of  $\mathcal{O}_K$ .

Fix such a base ring  $\mathcal{O} = \mathcal{O}_{K,S}$  from now on, and assume that the polynomials in (1) have coefficients in  $\mathcal{O}$ .

If  $R$  is any  $\mathcal{O}$ -algebra, the set of solutions of (1) with coordinates in  $R$  is denoted  $X(R)$ :

$$X(R) := \{(x_1, \dots, x_n) \in R^n \text{ satisfying (1)}\}.$$

The functor  $R \mapsto X(R)$  from the category of  $\mathcal{O}$ -algebras to the category of sets is *representable*,

$$(2) \quad X(R) = \text{Hom}_{\mathcal{O}}(A_X, R), \quad \text{where } A_X = \mathcal{O}[x_1, \dots, x_n]/(f_1, \dots, f_m).$$

In this way the system (1) determines the *affine scheme*  $X := \text{Spec}(A_X)$  over  $\text{Spec}(\mathcal{O})$ .

When the polynomials in (1) are homogeneous, it is customary to view  $X$  as giving rise to a *projective scheme* over  $\mathcal{O}$ . When  $R$  is a principal ideal domain, the set  $X(R)$  is a subset of the set  $\mathbb{P}_{n-1}(R)$  of  $n$ -tuples  $(x_1, \dots, x_n) \in R^n$  satisfying  $Rx_1 + \dots + Rx_n = R$ , taken modulo the equivalence relation defined by

$$(x_1, \dots, x_n) \sim (x'_1, \dots, x'_n) \quad \text{if } x_i x'_j - x_j x'_i = 0, \quad \forall \quad 1 \leq i, j \leq n.$$

Specifically,

$$X(R) := \{(x_1, \dots, x_n) \in \mathbb{P}_{n-1}(R) \text{ satisfying (1)}\}.$$

In the projective setting, replacing the base ring  $\mathcal{O}$  by its fraction field  $K$ , and  $X$  by its *generic fiber*  $X_K$ —a projective variety over  $K$ —does not change the Diophantine problem. For instance, the natural map  $X(\mathcal{O}) \rightarrow X_K(K)$  is a bijection. So there is no distinction between the study of integral and rational points on a scheme whose generic fiber is a projective variety.

Here are some of the basic questions that can be asked about the behaviour of  $X(\mathcal{O})$ .

QUESTION 1. *What is the cardinality of  $X(\mathcal{O})$ ? Is it finite, or infinite?*

QUESTION 2. *If  $X(\mathcal{O})$  is finite, can its cardinality be bounded by a quantity depending in a simple way on  $X$  and  $\mathcal{O}$ ?*

QUESTION 3. *Can  $X(\mathcal{O})$  be effectively determined?*

The arithmetic complexity of a point  $P \in X(\mathcal{O})$ —roughly speaking, the amount of space that would be required to store the coordinates of  $P$  on a computer—is measured by a (logarithmic) *height function*

$$h : X(\mathcal{O}) \rightarrow \mathbf{R}.$$

The precise definitions and basic properties of heights are discussed elsewhere in this volume. Let us just mention that for any real  $B > 0$ , the number  $N(X; B)$  of  $P \in X(\mathcal{O})$  with  $h(P) \leq B$  is finite, in any reasonable definition of  $h$ .

**QUESTION 4.** *When  $X(\mathcal{O})$  is infinite, what can be said about the asymptotics of the function  $N(X; B)$  as  $B \rightarrow \infty$ ?*

A related question is concerned with the *equidistribution* properties of the points in  $X(\mathcal{O})$  (ordered by increasing height), relative to some natural measure on  $X(\mathbf{R})$  or  $X(\mathbf{C})$ .

An *algebraic curve* over  $\mathcal{O}$  is a scheme  $X$  (either affine or projective) of relative dimension one over  $\text{Spec}(\mathcal{O})$ . If its generic fiber is smooth, the set  $X(\mathbf{C})$  (relative to a chosen embedding of  $\mathcal{O}$  into  $\mathbf{C}$ , through which  $\mathbf{C}$  becomes an  $\mathcal{O}$ -algebra) is a one-dimensional complex manifold. While a curve is often described by equations like (1), it is to be viewed up to isomorphism, as an equivalence class of such equations modulo suitable changes of variables. The main objects we will study are curves  $X$  over  $\text{Spec}(\mathcal{O})$ , and the behaviour of the sets  $X(R)$  as  $R$  ranges over different  $\mathcal{O}$ -algebras.

**Remark.** The term “integral points on elliptic curves” is often used (particularly by number theorists) to refer to the integral solutions of an affine Weierstrass equation:

$$E_0 : y^2 = x^3 + ax + b$$

which describes an *affine curve* over the base ring  $\mathbf{Z}[a, b]$ . This is an abuse of terminology, since elliptic curves are always defined as projective varieties by passing to the projective equation

$$E : y^2z = x^3 + axz^2 + bz^3,$$

resulting in the addition of the “point at infinity”  $O := (0, 1, 0)$  to  $E_0$ . This passage is crucial. Note, for instance, that  $E$  has the structure of an algebraic group, while  $E_0$  does not. It should be kept in mind that the common usage “integral points on  $E$ ” refers to the integral points on the affine curve  $E_0 = E - \{O\}$ , which is not an elliptic curve at all, and that, according to the definitions in standard usage,  $E(\mathcal{O})$  is equal to  $E(K)$  because  $E$  is projective.

### The fundamental trichotomy for curves

Suppose that the curve  $X$  is *generically smooth*, i.e., its generic fiber is a nonsingular curve over  $K$ , so that  $X(\mathbf{C})$  has the structure of a smooth Riemann surface. The set  $X(\mathbf{C})$  is (topologically and analytically) identified with

$$X(\mathbf{C}) \simeq S - \{P_1, \dots, P_s\},$$

where  $S$  is a compact Riemann surface (of genus  $g$ , say) and  $P_1, \dots, P_s$  are distinct points. The invariants  $g$  and  $s$ , which completely determine the topological isomorphism class of  $X(\mathbf{C})$ , can be packaged into the *Euler characteristic*

$$\chi(X) = 2 - 2g - s.$$

The answers to Questions 1–4 above depend on the sign of  $\chi(X)$  in an essential way.

**I. Positive Euler characteristic.** If  $\chi(X) > 0$ , then  $g = 0$  and  $s = 0$  or  $1$ . Therefore  $X$  is isomorphic over  $\bar{K}$  either to the projective line  $\mathbb{P}_1$  or the affine line