DE GRUYTER

Nikos Tzanakis

ELLIPTIC DIOPHANTINE EQUATIONS

A CONCRETE APPROACH VIA THE ELLIPTIC LOGARITHM

SERIES IN DISCRETE MATHEMATICS AND APPLICATIONS

DE G

Nikos Tzanakis

Elliptic Diophantine Equations

A Concrete Approach via the Elliptic Logarithm

De Gruyter

Mathematics Subject Classification 2010: 11D25, 11D41, 11D88, 11G05, 11G07, 11G50, 11H06, 11J86, 11Y16, 11Y50, 11-04, 14E05, 14H52, 14Q05, 33E05, 52C07, 68W30

Author
Nikos Tzanakis
University of Crete
Department of Mathematics
Voutes Campus
70013 Heraklion, Crete
Greece
tzanakis@math.uoc.gr

ISBN 978-3-11-028091-3
e-ISBN 978-3-11-028114-9
Set-ISBN 978-3-11-028115-6
ISSN 2195-5557

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.dnb.de.

Typesetting: PTP-Berlin Protago-TEX-Production GmbH, www.ptp-berlin.de
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen
♾ Printed on acid-free paper

Printed in Germany

www.degruyter.com

De Gruyter Series in Discrete Mathematics and Applications 2

Editor
Colva M. Roney-Dougal, St Andrews, United Kingdom

To my beloved wife Maro,
and to our family's younger mathematicians,
Eleni & Alexis, and Giorgos,
with whom I share in life mathematics and so much more.

Preface

This book 17 0 is about *elliptic Diophantine equations*, the most standard instance of such an equation being the equation $y^2 = x^3 + Ax + B$ in integers x, y, where $A, B \in \mathbb{Q}$ and the right-hand side has no multiple roots. Many more Diophantine equations are elliptic Diophantine equations; in Chapter 1 the term is explained in its generality.

More specifically, the main theme of this book is the *explicit resolution* of such equations and the resolution method that is exposed in detail is called *elliptic logarithm method* or, briefly, Ellog, in accordance with the terminology and notation introduced in [55]. The method has two main characteristics which are, first, the exploitation of the *group structure* with which the points of a non-singular cubic curve are endowed and, second, the use of *linear forms in elliptic logarithms*. The method owes its name to its second characteristic, the most modern. Immediately below we give more explanations.

The first main characteristic (or ingredient) of the Ellog, which makes possible the transition from the elliptic Diophantine equation to linear forms in elliptic logarithms – the second main characteristic – is the fact that, on the one hand, an elliptic Diophantine equation can be transformed, by an appropriate "change of variables", into a non-singular cubic equation of a special shape[1] and, on the other hand, that the set of points[2] of the curve defined by this cubic equation, is endowed with the structure of a finitely generated abelian group. The operation of "addition" in this group is a consequence of the simple observation that the third point of intersection with the curve of a line joining two points of the curve with coordinates in a number field also has coordinates in this same number field; if the two points coincide, as "the line joining them" we understand the tangent at the point. Thus, if we know two distinct rational, say, solutions (points), we can obtain a third one, also with rational coordinates, which is the third intersection with the curve of the line joining the two known points; and if we know only one solution (point), as a "line joining the two known points" we consider the tangent at the known point. This is the *chord and tangent* method for generating new solutions from known ones. At this point I refer the reader to the beautiful booklet of I. G. Bashmakova [3]. Bashmakova seems to believe that, in the two problems below, found in *Arithmetica*, Diophantus applied the chord and tangent method consciously. I am very cautious about this view; nevertheless, one *might ex-*

[1] The Weierstrass equation.

[2] With coordinates rational or, more generally, in a number field.

plain Diophantus's solution to these problems as an application of this method, which is what I do below, following Bashmakova's exposition [3, Chapter 6].

> Problem Δ-24 of Diophantus's *Arithmetica* [61, pp. 242–244].[3]
> *To divide a given number into two numbers such that their product is a cube minus its side.*
> Original text: Δοθέντα ἀριθμὸν διελεῖν εἰς δύο ἀριθμούς, καὶ ποιεῖν τὸν ὑπ' αὐτῶν κύβον παρὰ πλευράν.

Sketch, in modern language, of Diophantus's solution. As a "given number" he takes 6 and the two numbers in which 6 is "divided" are 6 and $6-x$. Let y be the "side of the cube", so that, by the problem, $x(6-x) = y^3 - y$. Diophantus puts $y = ax - 1$ with a temporarily not specified.[4] His first attempt, setting $a = 2$, is not successful because the coefficients of x are not cancelled out. Therefore he takes $a = 3$ and then his equation becomes $27x^3 - 26x^2 = 0$, which gives the non-zero solution $x = 26/27$, $y = 136/27$.

A deeper explanation of the above solution. Consider $x(6-x) = y^3 - y$ as a curve possessing the obvious point $(x, y) = (0, -1)$. The tangent to the curve at this point meets the curve at three points, two of them being $(0, -1)$ counted twice and the third will be the new sought-for point. The equation of the tangent is $y = 3x - 1$ and we are led to Diophantus's choice $a = 3$.
In this solution, only one point, namely $(0, -1)$, was a priori known, so that the tangent was used. An analogous use of tangent explains the *duplication formula* of Bachet (1621), by which he was able to find rational solutions (x, y) with $xy \neq 0$ to the equation $y^2 = x^3 + c$ for any integer $c \neq 1, -432$, once he knew one rational solution (x_1, y_1) with $x_1 y_1 \neq 0$; see [46, Introduction].

> Problem Δ-26 of Diophantus's *Arithmetica* [61, pp. 248–250].[5]
> *To find two numbers such that their product augmented by either gives a cube.*
> Original text: Νὰ εὑρεθῶσι δύο ἀριθμοί, ὅπως τὸ γινόμενον αὐτῶν σὺν ἑκάτερον σχηματίζει κύβον.

Sketch, in modern language, of Diophantus's solution. As the first number he takes a multiple of a cube;[6] specifically, $8x$. He takes the second number equal to $x^2 - 1$. The conditions of the problem require that both $8x(x^2-1) + 8x$ and $8x(x^2-1) + x^2 - 1$ be cubes. The first condition is satisfied by every x, while the second gives $8x^3 + x^2 - 8x -$

[3] Also [51, p. 199].
[4] "I form a cube by arbitrary times minus its side" is my rough translation from Greek of Diophantus's statement.
[5] Also [51, p. 203].
[6] "I form the first by an arbitrary cube" is my rough translation from Greek of Diophantus's statement.

$1 = y^3$. Again, Diophantus sets $y = 2x - 1$, obtaining thus the solution $x = 14/13$; hence the sought-for numbers are $8 \cdot 14/13 = 112/13$ and $(14/13)^2 - 1 = 27/169$.
A deeper explanation of the above solution. Why the substitution $y = ax - 1$ with $a = 2$? What is special about this value for a? In projective coordinates $(X : Y : Z)$ the above cubic equation becomes[7] $8X^3 + X^2Z - 8XZ^2 - Z^3 = Y^3$ and the equation of the above line through the point $(0, -1)$ – which is the projective point $(0 : -1 : 1)$ – is $Y = aX - Z$. On this line, the "point at infinity" is $(1 : a : 0)$, and the requirement that this be also a point on the cubic curve forces $a = 2$. Thus, the solution of Diophantus is the third point of intersection of the (projective) cubic curve with the (projective) line joining the points $(0 : -1 : 1)$ and $(1 : 2 : 0)$.

The necessary theory and tools related to the above are discussed mainly in *Chapter 1* and, also, in *Chapter 2*.

The second characteristic (or ingredient) relevant to the method from which this book takes its name, consists in the fact that to each elliptic Diophantine equation one or more linear forms in elliptic logarithms are attached, and the computation of upper and lower bounds for them is a major part of the method. The necessary theory and tools for this are developed in *Chapter 3*.

A first complete image of $\mathfrak{Ellog}$, in general, which results from the combination of the two ingredients, is given in *Chapter 4*. Specialising the application of $\mathfrak{Ellog}$ to various classes of elliptic Diophantine problems results in *Chapters 5, 6, 7*, and *8*. Each of these chapters leads up to a theorem furnishing an *upper bound* for the absolute value of the linear form L, involved in the Diophantine problem, in terms of a critical parameter $M > 0$.

In *Chapter 9*, a major step is achieved due to a Theorem of S. David [12], namely, a lower bound for $|L|$ (the same L as above), again in terms of M (the same M as above) is obtained. All quantities in both the upper and the lower bound of $|L|$, except for M, are *explicit*; moreover, as it will turn out, *the lower bound runs faster to infinity with M than the upper bound* and this fact clearly implies an *explicit upper bound for M*. Why is this important? At this point, it is not possible to explain in a few sentences, the meaning of M. For the present, the reader should consider that an *explicit bound* for M would reduce the resolution of the Diophantine problem to that of checking which lattice points in a hyper-cube of side $2M$ satisfy a certain condition. This is what I call in this book an *effective resolution* to the Diophantine problem. It is important to stress the fact that this checking can be performed in practice only if M is "very small"; this issue is discussed later in this preface.

Four specific examples corresponding, respectively, to Chapters 5, 6, 7, and 8 are discussed, resulting in explicit very large upper bounds for M; in all cases this is larger than 10^{40}.

Unfortunately, this is a general fact: In all specific Diophantine problems, the effective upper bound for M is so large (something of the size of 10^{30}, say, would be very

[7] On setting $x = X/Z$ and $y = Y/Z$.

"friendly") that, in practice, the checking of lattice points in the hyper-cube, mentioned a few lines above, is impossible.

Is it possible to reduce the upper bound of M to a manageable size (say of a few decades)? This would lead to an *explicit resolution* of the Diophantine problem. The answer is, in principle, positive due to a reduction method developed by B. M. M. de Weger [72], which is based on the LLL-basis reduction algorithm of Lenstra–Lenstra–Lovász [27]. *Chapter 10* presents everything related to the reduction of the upper bound of M. The reduction method is then applied to the examples of Chapter 9, leading to upper bounds for M at most 17. This small upper bound leads then, very easily, to the complete *explicit* solution.

The theoretical idea of the method[8] goes back to Lang [25], who also explains it in [26]; its brief explanation is found in [45, Chapter IX.5, "Linear forms in elliptic logarithm"]. The discussion so far and the contents of this book confirm that from theory to practice a long way had to be covered; the method became *practical* only in 1994, after the work of R. J. Stroeker and the author [54], and, independently, the work of J. Gebel, A. Pethő and H. G. Zimmer [15]. These two 1994 papers would not have appeared if the work of N. Hirata-Kohno [17] and S. David [12], on lower bounds of linear forms in elliptic logarithms, had not been previously published. In a correspondence[9] during 1991–1992, I asked S. David if he could make *explicit* the constants involved in the results of [17]; I am extremely grateful to him for his accepting my far from non-trivial "challenge", which turned out to be a really heavy work [12] of more than 130 pages! For a clear and relatively short description of the practical "1994 method" I refer to [50, Chapter XIII].

Chapter 11 is special. In it, the resolution of the Weierstrass elliptic equation in S-integers is discussed. What do we mean by S-integers? If S is a finite set of primes, an S-integer is, by definition, a rational number, with the property that the prime decomposition of its denominator allows only primes belonging to S; in particular, every usual (rational) integer is an S-integer.

One has to develop a theory of *p-adic elliptic logarithms* (with p a prime) for the points of an elliptic curve, in analogy with the theory of elliptic logarithms developed in Chapter 3; this is done in Section 11.1. In Section 11.2 *linear forms in p-adic elliptic logarithms* are introduced and the p-adic version of $\mathfrak{Ell}\mathfrak{log}$, is developed. This section is inspired by the papers of N. Smart [47] and Pethő–Zimmer–Gebel–Herrmann [36]; the second paper completes the project set up in the first paper. When [36] was published, no *explicit* lower bound for linear forms in p-adic elliptic logarithms – the analogue in the p-adic case of S. David's theorem – existed, except for that in [39] which, however, is applicable only to elliptic curves of rank at most two.[10] Therefore the authors of [36]

[8] Without its "details" ☺: Lower bounds for linear forms in elliptic logarithms, reduction process and, in general, all computational aspects.

[9] Handwritten letters of the good old days!

[10] This result is improved in [18], but still treats the case of two p-adic elliptic logarithms.

turned to the recent, for those days, paper [16]. Very recently,[11] N. H. Kohno released a valuable paper [19], in which "the p-adic analogue of S. David's theorem" is proved. This is what is used in Chapter 11 instead of [16]. I am grateful to Noriko, who, meeting my desire, worked hard in order to provide me with her theorem before the date that I had to send my manuscript to the editors.

The chapter includes a specific example with the primes $p = 2, 3, 5, 7$ involved.

About the style of the book. To what extent should my exposition take for granted standard (more or less) material found in the literature? I had this speculation mainly concerning Section 1.2 of Chapter 1, Chapters 2, 3 and 9, Section 10.1 of Chapter 10, and Section 11.1 of Chapter 11. My decisions are detailed below.

The basic theory of elliptic curves is so beautifully written in various text-books – few of them (only) are included in my bibliography –, that my hypothetical contribution could be described by $\epsilon + \infty$! Therefore, Section 1.2 of Chapter 1 includes only the very basic facts that will be needed and gives references.

For the theory of heights, in Chapter 2, only a moderate use of p-adic theory is required. I found that standard texts either include so much material that reference to them would disorientate (with respect to this book's aim) my reader, or they adopt a point of view not very appropriate for the present book, as they build the relevant theory by considering extensions of $\mathbb{Q}_p$.[12]

Concerning Weierstrass equations over $\mathbb{C}$ and $\mathbb{R}$ and the Weierstrass $\wp$-function, treated in Chapter 3, I do the following. Since the basic general theory is so neatly written, for example, in [1, Chapter 1], I decided that I need not provide any explanation. However, specialisation of the general theory to Weierstrass equations with real coefficients is absolutely necessary in order to build a *practical* theory of elliptic logarithms. I decided to discuss this issue, rather in detail, guided by my personal taste. I adopted a very classical point of view, mainly based on the old (still in print) nice book [73] and the personal notes of N. Kritikos from A. Hurwitz's 1916–1917 E. T. H. lectures on elliptic functions.[13]

The hard core of Chapter 9 is a special – very important though – case of Sinnou David's Theorem. As I already mentioned, this is the result of his memoir [12] of more than 130 pages. The theorem, in the form appropriate for the needs of this book (Theorem 9.1.2), is stated only and aspects of its application in practice are discussed.

For the applications of Chapter 10 the main tool is the reduction technique of B. M. M. de Weger [72], which is based on the LLL-algorithm [27]. The style of [72] is very appropriate for this book,[14] but discusses many more applications than those

[11] Actually, when I was ready to send my manuscript to the editors!

[12] For this book's purposes, working with non-archimedean absolute values on (finite) extensions of $\mathbb{Q}$ is much more appropriate.

[13] These notes in Greek [23], prepared by the late Dr. I. Ferentinou-Nikolakopoulou, circulated around 1980 in the Department of Mathematics of the University of Crete.

[14] Is it accidental that B. M. M. de Weger and I had a congenial collaboration for years?

needed here. Therefore, in Chapter 10, among other issues, I expose the reduction process focusing on the particular applications of the book.

In Section 11.1 of Chapter 11, p-adic elliptic logarithms and their linear forms play the fundamental role. The theory on which the construction of such logarithms is based is described in Chapter IV of J. Silverman's valuable book [45], though from a point of view somewhat more general than necessary for this book. What I decided to do was state only the absolutely necessary facts from Silverman's exposition "translated" into a language appropriate for practical applications.
As in the case with S. David's Theorem in Chapter 11, the very recent and extremely important theorem of N. Hirata-Kohno, mentioned before, is only stated in the form appropriate for the needs of this book (Theorem 11.2.5).

Although a main characteristic of the book is its use of computational methods, *it is not a book on Computational Number Theory*; issues such as – to mention only a few examples – the actual computation of Mordell–Weil bases, the search for rational points on elliptic curves up to a certain bound, the computation of canonical heights, various aspects of the implementation of the LLL-algorithm, and/or improvements of existing methods and algorithms, are beyond the scope of the book. To this "rule" I allowed three exceptions: In Chapter 3, first, I did not refrain from discussing in detail the actual computation of a fundamental pair of periods for a Weierstrass equation with real coefficients, an issue that fits very well in the framework of the chapter.[15] Second, again in Chapter 3, I did not resist the temptation to describe the very clever algorithm of D. Zagier [74] for the computation of elliptic logarithms. Third, in Chapter 8, I present an algorithm of J. Coates related to the computation of the coefficients of Puiseux series.

Suggestions for reading this book. The Diophantine problems treated in this book are classified to five classes: Weierstrass, quartic elliptic, simultaneous Pell, general elliptic, and Weierstrass in S-integers; let us use for these problems the symbols $\mathcal{P}_i$, where $i = 5, 6, 7, 8, 11$, respectively, with this numbering justified by the chapter where the corresponding problem is mainly (but not exclusively) discussed. Since $\mathfrak{Ellog}$ is applied in the most direct manner to $\mathcal{P}_4$, I would suggest that the reader starts by understanding the resolution of this problem. In general, in order to understand the complete and explicit resolution of problem $\mathcal{P}_i$, I suggest the following scheme:

- Read carefully Chapter 1.
- Make a first superficial reading of Chapter 2 to become acquainted with heights, so that you can read Section 2.6; if you already know about heights, go directly to Section 2.6.
- Pay attention to the content of Section 3.5. An understanding of the previous sections of Chapter 3 is necessary, with the exception of Section 3.4 which you will need only if you are interested in the actual computation of periods.

[15] Besides, a detailed treatment of this issue is not easily found in the literature.

- Comprehend the content of the short Chapter 4.
- Read carefully Chapter i. If i = 11 do not proceed to Theorem 11.2.6; instead, proceed to the following step.
- From Chapter 9 read carefully Sections 9.1 and 9.2.
  If i = 11 go back to Theorem 11.2.6 and complete your study of Chapter 11. END!
  If i is not 11, read that Section among 9.3, 9.4, 9.5 and 9.6 which corresponds to the chosen $\mathcal{P}_i$.
- If i is different from 11, proceed to Chapter 10, read Section 10.1 and chose among the subsections of Section 10.2 the one that corresponds to the chosen $\mathcal{P}_i$. END!

Software packages. My frequent reference to the software packages PARI (free), MAGMA and MAPLE is because I happen to have been acquainted with them for years. Alternatively, for the applications of this book, one could turn to SAGE (free). As this was developed very recently – comparatively to the previously mentioned packages –, I had not the time to gain experience with it; this is the only reason why SAGE is not mentioned in my applications.

Final acknowledgments. The materials of Chapters 4, 5, 8, 9 and 10 are mostly based on joint-papers with Roel Stroeker published between 1994 and 2003. It was a real pleasure to cooperate with Roel, noble friend and brave co-traveller in the long and adventurous but beautiful trip in the field of elliptic Diophantine equations.

Around that same period, other people worked independently on various aspects of elliptic Diophantine equations, from a similar point of view; I have in mind mainly (in alphabetic order) J. Gebel, E. Herrmann, A. Pethő, N. P. Smart and H. G. Zimmer. We always had fruitful, and friendly communication; also their work was an inspiration source in writing Chapter 11.

All serious computations in the examples of this book, besides their obvious debt to the software packages mentioned above, owe much, though indirectly, to people on whose work the routines that I have used are, more or less, based; let me mention (alphabetically) J. Cremona, M. van Hoeij, A. K. Lenstra, H. W. Lenstra, L. Lovász, J. Silverman, M. Stoll, B. M. M. de Weger, D. Zagier and many anonymous (to me, at least) heroes who are behind the algorithms' implementation in various packages.

Generally speaking, this book owes something to every author whose name appears in the bibliography; to some of them it owes much more, as becomes clear from the frequent references to their work. I also thank Y. Thomaidis who, shared with me his professional views about some issues of Diophantus's Arithmetica.

Warm thanks to De Gruyter for its continued collaboration and to D. Poulakis for inciting me to write this book and his warm encouragement.

I am grateful to P. Voutier for his careful reading of Chapters 2 and 3. Of course, I am absolutely responsible for anything wrong that possibly escaped his attention.

I am indebted to my wife Maro for her lifelong support, and for her warm encouragement and patience when I was writing this book; this has been a main factor for its completion!

Heraklion, Crete, May 12, 2013 Nikos Tzanakis

Contents

Chapter 1

Elliptic curves and equations

1.1 A general overview

In this section we make an overview of general facts, terminology and conventions that will be used in this book.

Let $g(X, Y)$ be a non-zero polynomial with coefficients in a subfield K of $\mathbb{C}$ (in most cases, $K = \mathbb{Q}$), irreducible over $\mathbb{C}$, and let R be a subring of K (usually, but not always, $R = \mathbb{Z}$) which will be fixed throughout this chapter. We are interested in solving the *Diophantine* equation

$$g(u, v) = 0, \quad (u, v) \in R \times R. \tag{1.1}$$

The characterisation of the above equation as "Diophantine" comes from the requirement that the unknowns u, v belong to the prescribed ring R and not to the whole $\mathbb{C}$ or $\mathbb{R}$. Solving the Diophantine equation is far different from solving the *algebraic* equation $g(u, v) = 0$, in which the unknowns belong to $\mathbb{C}$. The solutions of the *algebraic* equation define a curve or, more precisely, a *model* C of a curve; we state this by writing

$$C : g = 0; \quad g(X, Y) = \text{a specific polynomial in } X, Y$$

and we say that C or, more precisely, the model C is defined by the polynomial $g(X, Y)$, or by the equation $g = 0$. Thus, we view C as the set $C(\mathbb{C}) = \{(u, v) \in \mathbb{C} \times \mathbb{C} : g(u, v) = 0\}$ and the elements of $C(\mathbb{C})$ are called *points of (the model)* C. Sometimes we wish to focus our interest to the "real part" of C, which is the set $C(\mathbb{R}) = \{(u, v) \in \mathbb{R} \times \mathbb{R} : g(u, v) = 0\}$ of *real points* of (the model) C. In general, if A is a subring of $\mathbb{C}$, we set $C(A) = \{(u, v) \in A \times A : g(u, v) = 0\}$ and if $(u, v) \in C(A)$, we say that (u, v) is an A-point of (on) C. The fact that the model C is defined by means of the polynomial g, whose coefficients belong to R, is expressed by saying that C is *defined over* R.

Sometimes (actually very rarely) we will need to refer to the *projective equation* or, equivalently, to the *projective model* corresponding to equation (1.1). This results from the so-called *homogenisation* of the variables u and v, which consists in considering the equation

$$\begin{aligned} &\overline{g}(U : V : W) = 0, \\ &\overline{g}(U : V : W) \stackrel{\text{def}}{=} W^n g(U/W, V/W), \quad n = \max\{\deg_u g, \deg_v g\}. \end{aligned} \tag{1.2}$$

Note that $\overline{g}(U, V, W)$ is homogeneous in U, V, W of degree n and $\overline{g}(u : v : 1) = g(u, v)$.

If $\overline{g}(U : V : W) = 0$, then and only then $\overline{g}(kU : kV : kW) = 0$ for every $k \in \mathbb{C}^*$, therefore it is more appropriate to view the solutions of the equation $\overline{g}(U : V : W) = 0$ projectively, i.e. as points $(U : V : W) \in \mathbb{P}^2(\mathbb{C})$ rather than as solutions or affine points $(U, V, W) \in \mathbb{C}^3$. If $\overline{g}(U : V : W) = 0$ for some $(U : V : W) \in \mathbb{P}^2(\mathbb{C})$ and there exists a $k \in \mathbb{C}^*$ such that $kU, kV, kW \in R$, then $(U : V : W)$ is a projective solution (point) over R.

The *dehomogenisation* process from $\overline{g} = 0$ to $g = 0$ consists in dividing $\overline{g}(U, V, W) = 0$ through by W^n and putting $(U/W, V/W) = (u, v)$.

In the homogenisation process, from every solution (u, v) of $g = 0$ we obtain a projective solution $(u : v : 1)$ of $\overline{g} = 0$. In the dehomogenisation process, a solution $(U : V : W)$ of $\overline{g} = 0$ furnishes a solution (u, v) of $g = 0$ if, and only if, $W \neq 0$, the solution in this case being $(u, v) = (U/W, V/W)$; but projective solutions of the form $(U : V : 0)$ cannot be "dehomogenised" to solutions (u, v) of (1.1). Such solutions $(U : V : 0)$ are characterised as *solutions (points) at infinity* of the equation (1.1).

Now we proceed to discussing the important fact that different equations may define the same *curve*. In order to make this more precise, we need first the following definition:

Definition 1.1.1. For $i = 1, 2$, let $g_i(X, Y)$ be non-zero polynomials in $\mathbb{C}[X, Y]$, irreducible over $\mathbb{C}$ and consider the models $C_i : g_i = 0$.

We say that a birational transformation exists between C_1 and C_2 or, equivalently, that the models C_1 and C_2 are birationally equivalent if, for $(i, j) = (1, 2), (2, 1)$, rational functions $\mathcal{U}_{ij}, \mathcal{V}_{ij} \in \mathbb{C}(X, Y)$ exist such that: for (i, j) as above, if $(u_i, v_i) \in C_i(\mathbb{C})$ and we define $(u_j, v_j) = (\mathcal{U}_{ij}(u_i, v_i), \mathcal{V}_{ij}(u_i, v_i))$, then $(u_j, v_j) \in C_j(\mathbb{C})$ and $(\mathcal{U}_{ji}(u_j, v_j), \mathcal{V}_{ji}(u_j, v_j)) = (u_i, v_i)$.

Actually, the above definition of birational equivalence, though satisfactory for the needs of this book, is not very precise: What about points $(u_i, v_i) \in C_i(\mathbb{C})$ for which $\mathcal{U}_{ij}(u_i, v_i)$ or $\mathcal{V}_{ij}(u_i, v_i)$ is not defined (i.e. (u_i, v_i) is a zero of the denominator)? We overcome these difficulties if, for any model $C : g = 0$, we consider its *function field* $\mathbb{C}(C)$ (see a few lines below) and we define the notion of birational equivalence of two models C_1 and C_2 by means of their function fields $\mathbb{C}(C_1)$ and $\mathbb{C}(C_2)$. The function field of the model $C : g = 0$ is, by definition, the field $\mathbb{C}(\xi, \eta)$, where ξ is transcendental over $\mathbb{C}$ and η is algebraic over $\mathbb{C}(\xi)$, satisfying $g(\xi, \eta) = 0$. Equivalently, $\mathbb{C}(C)$ can be defined as the quotient field of the integral domain $\mathbb{C}[X, Y]/I$, where I is the ideal $g(X, Y)\mathbb{C}[X, Y]$ of $\mathbb{C}[X, Y]$. If two models C_1 and C_2 are birationally equivalent, then there exists an isomorphism of their function fields which fixes $\mathbb{C}$. For a treatment of these issues, very appropriate for the theoretical background of this book, we refer the reader to §§3,4 of the classical book [66]. For an alternative, or complementary, exposition the interested reader can refer to [45, Chapters I, II.1, II.2].