
Introduction

Mathematics, possibly due to its intrinsic abstraction, is considered to be a merely intellectual subject, and therefore extremely remote from everyday human activities. Surprisingly, this idea is sometimes found not only among laymen, but among working mathematicians as well. So much so that mathematicians often talk about *pure mathematics* as opposed to *applied mathematics* and sometimes attribute to the former a questionable birthright.

On the other hand, it has been remarked that those two categories do not exist but, just as we have good and bad literature, or painting, or music, so we have *good* or *bad* mathematics: the former is applicable, even if at first sight this is not apparent, in any number of fields, while the latter is worthless, even within mathematics itself. However, one must recognise the truth in the interesting sentence with which two of our colleagues, experts about applications, begin the preface to the book [47]: *In theory there is no difference between theory and practice. In practice there is.*

We believe that this difference cannot be ascribed to the intrinsic nature of mathematical theories, but to the stance of each single mathematician who creates or uses these theories. For instance, until recently the branch of mathematics regarded as the closest to applications was undoubtedly mathematical analysis and especially the theory of differential equations. The branches of mathematics supposed to be farthest from applications were algebra and number theory. So much so that a mathematician of the calibre of G. H. Hardy claimed in his book [25] the supremacy of number theory, which was to be considered the true *queen* of mathematics, precisely due to its distance from the petty concerns of everyday life. This made mathematics, in his words, “gentle and clean”. A strange opinion indeed, since the first developments of algebra and number theory among the Arabs and the European merchants in the Middle Ages find their motivation exactly in very concrete problems arising in business and accountancy.

Hardy’s opinion, dating back to the 1940s, was based upon a prejudice, then largely shared among scientists. It is quite peculiar that Hardy did not know, or pretended not to know, that A. Turing, whom he knew very well, had

used that very mathematics he considered so detached to break the Enigma code, working for English secret services, dealing a deadly blow to German espionage (cf. [28]). However, the role played by algebra and number theory in military and industrial cryptography is well known from time immemorial. Perhaps Hardy incorrectly believed that the mathematical tools then used in cryptography, though sometimes quite complex, were nevertheless essentially elementary, not more than combinatorial tricks requiring a measure of extemporaneous talent to be devised or cracked, but leading to no solid, important, and enduring theories.

The advances in computer science in the last sixty years have made cryptography a fundamental part of all aspects of contemporary life. More precisely, cryptography studies transmission of data, coded in such a way that authorised receivers only may decode them, and be sure about their provenience, integrity and authenticity. The development of new, non-classical cryptographic techniques, like public-key cryptography, have promoted and enhanced the applications of this branch of the so-called *discrete mathematics*, which studies, for instance, the enumeration of symbols and objects, the construction of complex structures starting with simpler ones, and so on. Algebra and number theory are essential tools for this branch of mathematics, which is in a natural way suitable for the workings of computers, whose language is intrinsically *discrete* rather than *continuous*, and is essential in the construction of all security systems for data transmission. So, even if we are not completely aware of it, each time we use credit cards, on-line bank accounts or e-mail, we are actually fully using algebra and numbers. But there is more: the same techniques have been applied since the 1940s to the transmission of data on channels where interference is present. This is the subject of the theory of error-correcting codes which, though unwittingly, we use daily in countless ways: for instance when we listen to music recorded on a CD or when surfing the Web.

This textbook originated from the teaching experience of the authors at the University of Rome “Tor Vergata” where, in the past years, they taught this subject to Mathematics, Computer Science, Electronic Engineering and Information Technology students, as well as for the “Scuola di Insegnamento a Distanza”, and at several different levels. They gave courses with a strong algebraic or geometric content, but keeping in mind the algorithmic and constructive aspects of the theories and the applications we have been mentioning.

The point of view of this textbook is to be *friendly* and *elementary*. Let us try to explain what we mean by these terms.

By *friendly* we mean our attempt to always give motivations of the theoretical results we show to the reader, by means of examples we consider to be simple, meaningful, sometimes entertaining, and useful for the applications. Indeed, starting from the examples, we have expounded the general methods of resolution of problems that only apparently look different in form, setting and language. With this in mind, we have aimed to a simple and colloquial

style, while never losing sight of the formal rigour required in a mathematical treatise.

By *elementary* we mean that we assume our readers to have a quite limited background in basic mathematical knowledge. As a rule of the thumb, a student having followed a good first semester in Mathematics, Physics, Computer Science or Engineering may confidently venture through this book. However, we have tried to make the treatment as self-contained as possible regarding the elements of algebra and number theory needed in cryptography and coding theory applications. *Elementary*, however, does not mean *easy*: we introduced quite advanced concepts, but did so gradually and always trying to accompany the reader, without assuming previous advanced knowledge.

The starting point of this book is the well-known set of integer numbers and their *arithmetic*, that is the study of the operations of addition and multiplication. Chapter 1 aims to make the reader familiar with integer numbers. Here mathematical induction and recursion are covered, giving applications to several concrete problems, such as the analysis of dynamics of populations with assigned reproduction rules, the computation of numbers of moves in several games, and so on. The next topics are divisions, the greatest common divisor and how to compute it using the well-known Euclidean algorithm, the resolution of Diophantine equations, and numeral systems in different bases. These basic notions are first presented in an elementary way and then a more general theoretical approach is given, by introducing the concept of Euclidean ring. The last part of the chapter is devoted to continued fractions.

One of the goals of Chapter 1 is to show how, in order to solve concrete problems using mathematical methods, the first step is to build a *mathematical model* that allows a translation into one or more mathematical problems. The next step is the determination of suitable *algorithms*, that is procedures consisting of a finite sequence of *elementary operations* yielding the solution to the mathematical problems describing the initial question. In Chapter 2 we discuss the fundamental concept of *computational complexity* of an algorithm, which basically counts the elementary operations an algorithm consists of, thus evaluating the time needed to execute it. The importance of this concept is manifest: among the algorithms we have to distinguish the feasible ones, that is those executable in a sufficiently short time, and the unfeasible ones, due to the time needed for their execution being too long independently of the computing device used. The algorithms of the first kind are the *polynomial* ones, while among those of the second kind there are, for instance, the *exponential* ones. We proceed then to calculate the complexity of some fundamental algorithms used to perform elementary operations with integer numbers.

In Chapter 3 we introduce the concept of congruence, which allows the passage from the infinite set of integer numbers to the finite set of residue classes. This passage from infinite to finite enables us to implement the elementary operations on integers in computer programming: a computer, in fact, can work on a finite number of data only.

Chapter 4 is devoted to the fundamental problem of factoring integer numbers. So we discuss prime numbers, which are the building blocks of the structure of integer numbers, in the sense that each integer number may be represented as a product of prime numbers: this is the so-called *factorisation* of an integer number. Factoring an integer number is an apparently harmless problem from a theoretical viewpoint: the factorisation exists, it is essentially unique, and it can be found by the famous *sieve of Eratosthenes*. We show, however, the unfeasibility of this exponential algorithm. For instance, in 1979 it has been proved that the number $2^{44497} - 1$, having 13395 decimal digits, is prime: by using the sieve of Eratosthenes, it would take a computer executing one million multiplications per second about 10^{6684} years to get this result! The modern public-key cryptography, covered in Chapter 7, basically relies on the difficulty of factoring an integer number. In Chapter 4 elements of the general theory of factorial rings can also be found, in particular as regards its application to polynomials.

In Chapter 5 finite fields are introduced; they are a generalisation of the rings of residue classes of integers modulo a prime number. Finite fields are fundamental for the applications to cryptography and codes. Here we present their main properties, expounded with several examples. We give an application of finite fields to the resolution of polynomial Diophantine equations. In particular, we prove the law of quadratic reciprocity, the key to solving second degree congruences.

In Chapter 6 most of the theory presented so far is applied to the search for *primality tests*, that is algorithms to determine whether a number is prime or not, and for factorisation methods more sophisticated than the sieve of Eratosthenes; even if they are in general exponential algorithms, just like Eratosthenes', in special situations they may become much more efficient. In particular, we present some primality tests of probabilistic type: they are able to discover in a very short time whether a number has a high probability of being a prime number. Moreover, we give the proof of a recent polynomial primality test due to M. Agrawal, N. Kayal and N. Saxena; its publication has aroused a wide interest among the experts.

Chapter 7 describes the applications to cryptography. Firstly, we describe several classical cryptographic methods, and discuss the general laying out of a cryptographic system and the problem of cryptanalysis, which studies the techniques to break such a system. We introduce next the revolutionary concept of public-key cryptography, on which the transmission of the bulk of confidential information, distinctive of our modern society, relies. We discuss several public-key ciphers, main among them the well-known *RSA* system, whose security relies on the computational difficulty of factoring large numbers, and some of its variants making it possible, for instance, the electronic authentication of signatures. Recently new frontiers for cryptography, especially regarding security, have been opened by the interaction of classical algebra and arithmetic with ideas and concepts originating from algebraic geometry, and especially the study of a class of plane curves known as *elliptic*

curves. At the end of the chapter an introduction to these important developments is given.

Chapter 8 presents an introduction to coding theory, already mentioned above. This is a recent branch of mathematics in which sophisticated combinatorial, algebraic and geometric techniques converge, in order to study the mathematical aspects of the problem of transmitting data through noisy channels. In other words, coding theory studies techniques to send data through a channel when we give for granted that some errors will happen during transmission. These techniques enable us to correct the errors that might arise, as well as to quickly encode and decode the data we intend to send.

In Chapter 9 we give a quick glance at the new frontiers offered by *quantum cryptography*, which relies on ideas originating in *quantum mechanics*. This branch of physics makes the creation of a *quantum computer* at least conceivable; if such a computer were actually built, it could execute in polynomial time computations a usual computer would need an exponential time to perform. This would make all present cryptographic systems vulnerable, seriously endangering civil, military, financial security systems. This might result in the collapse of our civilisation, largely based on such systems. On the other hand, by its very nature, the concept of a quantum computer allows the design of absolutely unassailable *quantum cryptographic systems*, even by a quantum computer; furthermore, such systems have the astonishing property of being able to detect if eavesdroppers attempt, even unsuccessfully, to hear in on a restricted communication.

Each chapter is followed by an appendix containing:

- a list of exercises on the theory presented there, with several levels of difficulty; in some of them proofs of supplementary theorems or alternative proofs of theorems already proved in the text are given;
- a list of exercises from a computational viewpoint;
- suggestions for programming exercises.

The most difficult exercises are marked by an asterisk. At the end of the book many of the exercises are solved, especially the hardest theoretical ones.

Some sections of the text may be omitted in a first reading. They are set in a smaller type, and so are the appendices.

We wrote this book having in mind students of Mathematics, Physics, Computer Science, Engineering, as well as researchers who are looking for an introduction, without entering in too many details, to the themes we have quickly described above.

In particular, the book can be useful as a complementary text for first and second year students in Mathematics, Physics or Computer Science taking a course in Algebra or Discrete Mathematics. In Chapters 1, 3, and 4 they will find a concrete approach, with many examples and exercises, to some basic algebraic theories. Chapters 5 and 6, though more advanced, are in our opinion within the reach of a reader of this category.

The text is particularly suitable for a second or third year course giving an introduction to cryptography or to codes. Students of such a course will probably already have been exposed to the contents of Chapters 1, 3, and 4; so teachers can limit themselves to quick references to them, suggesting to the students only to solve some exercises. They can then devote more time to the material from Chapter 5 on, and particularly to Chapter 7, giving more or less space to Chapters 8 and 9.

The bibliography lists texts suggested for further studies in cryptography and codes, useful for more advanced courses.

A first version of this book, titled “Note di matematica discreta”, was published in 2002 by Aracne; we are very grateful to the publishers for their permission for the publication of this book. This edition is widely expanded and modified: the material is presented differently, several new sections and in-depth analysis have been added, a wider selection of solved exercises is offered.

Lastly, we thank Dr Alberto Calabri for supervising the layout of the book and the editing of the text, especially as regards the exercise sections.

Rome,
August 2008

M. Welleda Baldoni
Ciro Ciliberto
Giulia Maria Piacentini Cattaneo



<http://www.springer.com/978-3-540-69199-0>

Elementary Number Theory, Cryptography and Codes

Baldoni, M.W.; Ciliberto, C.; Piacentini Cattaneo, G.M.

2009, XVI, 522 p. 10 illus., Softcover

ISBN: 978-3-540-69199-0