# Advanced Topics in Computational Number Theory

by

Henri COHEN

Version of August 27, 1998

*This manuscript was typed using LaTeX and the Springer-Verlag* `clmono01` *macropackage.*

## Preface

The computation of invariants of algebraic number fields such as integral bases, discriminants, prime decompositions, ideal class groups and unit groups, is important both for its own sake, and for the numerous applications that it has, for example to the solution of Diophantine equations. The practical completion of this task (sometimes known as the Dedekind program) has been one of the major achievements of computational number theory in the past ten years, thanks to the efforts of many people. Even though some practical problems still exist, one can consider the subject as solved in a satisfactory manner, and it is now routine to ask a specialized Computer Algebra System such as Kant/Kash, LiDIA, Magma or Pari/GP, to perform number field computations which would have been unfeasible only ten years ago. The (very numerous) algorithms which are used are essentially all described in "A Course in Computational Algebraic Number Theory", GTM 138, first published in 1993 (third corrected printing 1996), which will be referred to as [Coh0], which also treats other subjects such as elliptic curves, factoring and primality testing.

It is important and natural to generalize these algorithms. Several generalizations can be considered, but the most important are certainly the generalizations to global function fields (finite extensions of the field of rational functions in one variable over a finite field), and to relative extensions of number fields. As in [Coh0], in the present book we will only consider number fields and not deal at all with function fields.

We will thus address some specific topics related to number fields, and there is no attempt to be exhaustive in the choice of subjects. The topics have been chosen primarily because of my personal tastes, and of course because of their importance. Almost all of the subjects which are discussed in this book are quite new from the algorithmic aspect (usually post 1990), and almost all of the algorithms have been implemented and tested in the number theory package Pari/GP (see [Coh0] and [BBBCO]). The fact that the subjects are new does not mean that they are more difficult. In fact, as the reader will see when reading this book in depth, the algorithmic treatment of certain parts of number theory which have the reputation of being "difficult", is in fact much *easier* than the theoretical treatment. A case in point is computational class field theory (see Chapter 4). I do not mean that the proofs become any simpler, but only that one gets a much better grasp on the subject by studying its algorithmic aspects.

As already mentioned, a common point to most of the subjects discussed in this book is that we will deal with *relative* extensions, but we will also study other subjects. We will see that most of the algorithms given in [Coh0] for the absolute case can be generalized to the relative case.

The book is organized as follows. Chapters 1 and 2 contain the theory and algorithms concerning Dedekind domains and relative extensions of number fields, and in particular the generalization to the relative case of the round 2 and related algorithms.

Chapters 3, 4, 5 and 6 contain the theory and complete algorithms concerning class field theory over number fields. The highlights are the algorithms for computing the structure of $(\mathbb{Z}_K/\mathfrak{m})^*$, of ray class groups, and relative equations for Abelian extensions of number fields using Kummer theory, Stark's conjectures and complex multiplication. The reader is warned that Chapter 5 is rather technical, but contains a wealth of information useful both for further research and for any serious implementation. On the other hand, the analytic techniques using Stark's conjecture or complex multiplication described in Chapter 6 are fascinating since they construct purely algebraic objects using analytic means.

Chapters 1 to 6 form a homogeneous subject matter which can be used for a 6 month to 1 year advanced graduate course in computational number theory, omitting perhaps the most technical parts of Chapter 5.

The subsequent chapters deal with more miscellaneous subjects. In Chapter 7, we consider other variants of the notions of class and unit groups, such as relative class and unit groups or $S$-class and unit groups. We sketch an algorithm which allows the direct computation of relative class and unit groups, and give applications of $S$-class and unit groups to the algorithmic solution of norm equations, due to D. Simon.

In Chapter 8, we explain in detail the correspondence between cubic fields and binary cubic forms, discovered by H. Davenport and H. Heilbronn, and the important algorithmic consequences discovered by K. Belabas.

In Chapter 9, we give a detailed description of known methods for constructing tables of number fields or number fields of small discriminant, either by using absolute techniques based on the geometry of numbers, or using relative techniques based either on the geometry of numbers or on class field theory.

In Appendix A, we give and prove a number of important miscellaneous results which can be found scattered in the literature but which are used in the rest of the book.

In Appendix B, we give an updated but much shortened version of [Coh0, Appendix A] concerning packages for number theory, and other useful electronic information.

In Appendix C, we give a number of useful tables which can be produced using the results of this book.

The book ends with an index of notations, an index of algorithms and a general index.

The present book is almost entirely self contained. Although numerous references are made to the algorithms contained in [Coh0], these can be considered as "black boxes" and used as such. It would be however preferable for the reader at some point to study some of the algorithms of [Coh0], in particular those which are generalized here.

**WARNINGS.**

(1) As usual, neither the author nor Springer-Verlag can assume any responsibility for consequences arising from the use of the algorithms given in this book.

(2) The author would also like to hear about errors, typographical or otherwise. Please send e-mail to

`cohen@math.u-bordeaux.fr`

Lists of known errors, both for [Coh0] and for the present book, can either be obtained by anonymous ftp from the URL

`ftp://megrez.math.u-bordeaux.fr/pub/cohenbook`

or obtained through the author's home page on the Web at the URL

`http://www.math.u-bordeaux.fr/~cohen`

(3) There is however another important warning that was almost not relevant in [Coh0]. Almost all of the algorithms or the algorithmic aspects presented in this book are new, and most have never been published before or are being published while this book is going to press. Therefore it is quite possible that major mistakes are present, although this possibility is largely diminished by the fact that almost all of the algorithms have been tested, although not always thoroughly. More probably, certain algorithms can probably be radically improved. Evidently, the contents of this book only reflects the knowledge of the author at the time of writing.

## Acknowledgments

First of all, I would like to thank my colleagues Francisco Diaz y Diaz and Michel Olivier, with whom I have the pleasure of working every day, and who collaborated with me on the discovery and implementation of many of the algorithms described in this book. Secondly, I would like to thank Jacques Martinet, head of our Laboratoire, who has enormously helped by giving me an ideal working environment. Thirdly, my former students Karim Belabas, Jean-Marc Couveignes, Denis Simon and Emmanuel Tollis, who also contributed to part of the algorithms described here, as well as Xavier Roblot for everything related to Stark's conjectures.

In particular Karim Belabas is to be thanked for the contents of Chapter 8 which are mainly due to him, for having carefully read the manuscript of this book, and not least for having taken the ungrateful job of managing the Pari software, after making thorough modifications leading to version 2.

I would also like to thank Mehpare Bilhan and the Middle East Technical University (METU) in Ankara, Turkey, for having given me an opportunity to write a first version of part of the subjects treated in this book, which appeared as an internal report of METU in 1997.

Last but not least, I thank all our funding agencies, and in particular the C.N.R.S., the Ministry of Education and Research, the Ministry of Defense, the University Bordeaux I and the Région Aquitaine.

# Table of Contents