Advanced Topics in Computational Number Theory

Henri Cohen

This book is a sequel to the author's earlier work *A Course in Computational Algebraic Number Theory* which first appeared in 1993, and immediately became the definitive reference work in the field, with second and third printings in 1994 and 1996. Each runs to well over 500 pages, and includes a large number of algorithms given in detail, both special-purpose and more general, with a wealth of information and insight from the author's extensive first-hand experience. Together they form a extremely important and useful resource.

The first book (ACCANT for short) is broadly divided into three interlinked areas. Firstly, there are chapters on fundamental algorithms in elementary number theory, linear algebra (over $\mathbf{Z}$ and $\mathbf{Q}$) and for polynomials in one variable. These are all used constantly in the remaining parts: on algorithms for algebraic number fields (three chapters) and factorization and primality testing (one chapter each). There is also a chapter on elliptic curves, with some algorithms, to underpin later discussion of the elliptic curve method for integer factorization (ECM). This book was the outcome of the work carried out by the author and his collaborators in $\mathrm{A}^2\mathrm{X}$, the Laboratoire Algorithmique Arithmétique Experimentale at the University of Bordeaux. This group has also developed the PARI/GP software package, which originated as a testbed for the algorithms which they were developing in order to study systematically the arithmetic of number fields.

This second volume, *Advanced Topics in Computational Number Theory* (or ATCNT for short), continues in the same tradition. It contains detailed descriptions of many new algorithms for studying the arithmetic of number fields, as developed in Bordeaux and implemented in the more recent versions of PARI/GP. Again, the subject matter can be divided into approximately three parts, though this is somewhat arbitrary. The main new element, which was largely absent from ACCANT, is an emphasis on relative extensions: number fields L which are considered not as absolute extensions $L/\mathbf{Q}$, but as extensions of some intermediate field K. The benefit of this approach is to make tractable the study of (some) fields of much larger degree than could be tackled using the absolute algorithms of ACCANT. There is, unsurprisingly, a price to pay: the ring of integers of the ground field K is no longer $\mathbf{Z}$ but a more general Dedekind Domain $\mathbf{Z}_K$, where (in general) we no longer have unique factorization. One of the impressive achievements of the author is to show that, if handled properly, the algorithmic treatment of finitely-generated projective modules over a Dedekind Domain is just as practical as the theory of finitely-generated abelian groups. The foundation for this is laid in the first chapter (Fundamental Results and Algorithms in Dedekind Domains), which leads into the second chapter on relative number field algorithms. These foundations are likely to have more applications in other areas, such as an algorithmic treatment of function fields.

The best-understood relative extensions are of course the abelian extensions, which are completely determined, at least in theory, by Class Field Theory (CFT). The next four chapters, which form the heart of the book, contain a complete solution to the question of constructing class fields algorithmically. In fact, CFT itself is developed from first principles in Chapter 3, in a form and language more amenable to computation than in traditional treatments, so that ATCNT could be used as a reference source for concrete CFT. Most results of CFT (though not the deepest ones such as Takagi's Existence

Theorem) are proved here. Putting the theory into algorithmic practice involves a number of ideas which will have more applications than are seen here, such as the section on algorithms for finite abelian groups in Chapter 4. Two different methods are presented for constructing class fields explicitly from a given ground field and modulus: Kummer Theory in Chapter 5, and analytic methods in Chapter 6. For example, Chapter 6 shows how to use Stark Units for this: though Stark's conjecture is not proved, it can of course be assumed in order to carry out a construction which can then be verified afterwards. This is joint work with Roblot.

The last three chapters are more miscellaneous, covering a variety of topics, some of which could have been included already in ACCANT. The concepts of S-integers and S-units are treated algorithmically, with applications to the solution of norm equations (work of Simon). Chapter 8, on Cubic Number Fields, contains work of the author with another of his students, Belabas, which allows for a systematic study of all cubic fields almost as easily as for quadratic fields. The more general problem of systematically listing all number fields of given degree (or given signature) and discriminant within a given bound is the topic of the final chapter. This includes a section on quartic fields, which has already been superseded by more recent work of the Bordeaux group, and will, we understand, be the subject of a monograph currently in preparation.

As well as the nine chapters discussed so far, there are three appendices. The first covers some theoretical background (ramification theory, Kummer theory, and Dirichlet series); Secondly, the section on Electronic Information updates the shorter similar section in ACCANT with usefully annotated information on general and special computer packages, databases, mailing lists and web sites. Finally, a series of tables of number fields is given, as a taster for the far more extensive tables which are available online from the Bordeaux web site. There is an extensive bibliography, and separate indices of Notation and Algorithms as well as a general index.

The style of writing is concise though clear; I spotted very few misprints, and note that the author maintains a web site for the book from which up-to-date errata may be obtained.

The work involved in designing and implementing the algorithms described in these two books represents a monumental effort by the Bordeaux team, involving substantial theoretical investigations as well as the less highbrow (but crucial) activities of efficient programming implementation. In a sense, however, all this work has been preparatory. The fundamental desire is to study number fields, their arithmetic and inter-relationships. Throughout the history of the subject, these investigations have been based on substantial computations of examples and special cases. Without adequate computational tools, such as the ones being developed by the author and his colleagues, it is almost impossible to go beyond the study of quadratic and cyclotomic fields. The current generation of number theorists is extremely fortunate to have at its disposal several computer packages, such as PARI/GP, written by expert mathematicians, which make possible a wide range of investigations which an earlier generation could have only dreamt of. Cohen's two books are an essential guide to the intelligent use of these systems in serious research, as well as containing mathematics which is interesting, elegant and useful, and can be recommended most strongly.

J. E. Cremona, July 2000