Preface

Elementary number theory is concerned with the arithmetic properties of the ring of integers, $\mathbb{Z}$, and its field of fractions, the rational numbers, $\mathbb{Q}$. Early on in the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}[T]$, the ring of polynomials over a finite field. Both rings are principal ideal domains, both have the property that the residue class ring of any non-zero ideal is finite, both rings have infinitely many prime elements, and both rings have finitely many units. Thus, one is led to suspect that many results which hold for $\mathbb{Z}$ have analogues of the ring A. This is indeed the case. The first four chapters of this book are devoted to illustrating this by presenting, for example, analogues of the little theorems of Fermat and Euler, Wilson's theorem, quadratic (and higher) reciprocity, the prime number theorem, and Dirichlet's theorem on primes in an arithmetic progression. All these results have been known for a long time, but it is hard to locate any exposition of them outside of the original papers.

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions K of $\mathbb{Q}$, which are called algebraic number fields, and investigating properties of the ring of algebraic integers $O_K \subset K$, defined as the integral closure of $\mathbb{Z}$ in K. Similarly, we can consider $k = \mathbb{F}(T)$, the quotient field of A and finite algebraic extensions L of k. Fields of this type are called algebraic function fields. More precisely, an algebraic function fields with a finite constant field is called a global function field. A global function field is the true analogue of algebraic number field and much of this book will be concerned with investigating properties of global function fields. In Chapters 5 and 6, we will discuss function

fields over arbitrary constant fields and review (sometimes in detail) the basic theory up to and including the fundamental theorem of Riemann-Roch and its corollaries. This will serve as the basis for many of the later developments.

It is important to point out that the theory of algebraic function fields is but another guise for the theory of algebraic curves. The point of view of this book will be very arithmetic. At every turn the emphasis will be on the analogy of algebaic function fields with algebraic number fields. Curves will be mentioned only in passing. However, the algebraic-geometric point of view is very powerful and we will freely borrow theorems about algebraic curves (and their Jacobian varieties) which, up to now, have no purely arithmetic proof. In some cases we will not give the proof, but will be content to state the result accurately and to draw from it the needed arithmetic consequences.

This book is aimed primarily at graduate students who have had a good introductory course in abstract algebra covering, in addition to Galois theory, commutative algebra as presented, for example, in the classic text of Atiyah and MacDonald. In the interest of presenting some advanced results in a relatively elementary text, we do not aspire to prove everything. However, we do prove most of the results that we present and hope to inspire the reader to search out the proofs of those important results whose proof we omit. In addition to graduate students, we hope that this material will be of interest to many others who know some algebraic number theory and/or algebraic geometry and are curious about what number theory in function field is all about. Although the presentation is not primarily directed toward people with an interest in algebraic coding theory, much of what is discussed can serve as useful background for those wishing to pursue the arithmetic side of this topic.

Now for a brief tour through the later chapters of the book.

Chapter 7 covers the background leading up to the statement and proof of the Riemann-Hurwitz theorem. As an application we discuss and prove the analogue of the ABC conjecture in the function field context. This important result has many consequences and we present a few applications to diophantine problems over function fields.

Chapter 8 gives the theory of constant field extensions, mostly under the assumption that the constant field is perfect. This is basic material which will be put to use repeatedly in later chapters.

Chapter 9 is primarily devoted to the theory of finite Galois extensions and the theory of Artin and Hecke L-functions. Two versions of the very important Tchebatorov density theorem are presented: one using Dirichlet density and the other using natural density. Toward the end of the chapter there is a sketch of global class field theory which enables one, in the abelian case, to identify Artin L-series with Hecke L-series.

Chapter 10 is devoted to the proof of a theorem of Bilharz (a studentof Hasse) which is the function field version of Artin's famous conjecture on

primitive roots. This material, interesting in itself, illustrates the use of many of the results developed in the preceding chapters.

Chapter 11 discusses the behavior of the class group under constant field extensions. It is this circle of ideas which led Iwasawa to develop "Iwasawa theory," one of the most powerful tools of modern number theory.

Chapters 12 and 13 provide an introduction to the theory of Drinfeld modules. Chapter 12 presents the theory of the Carlitz module, which was developed by L. Carlitz in the 1930s. Drinfeld's papers, published in the 1970s, contain a vast generalization of Carlitz's work. Drinfeld's work was directed toward a proof of the Langlands' conjectures in function fields. Another consequence of the theory, worked out separately by Drinfeld and Hayes, is an explicit class field theory for global function fields. These chapters present the basic definitions and concepts, as well as the beginnings of the general theory.

Chapter 14 presents preliminary material on S-units, S-class groups, and the corresponding L-functions. This leads up to the statement and proof of a special case of the Brumer-Stark conjecture in the function field context. This is the content of Chapter 15. The Brumer-Stark conjecture in function fields is now known in full generality. There are two proofs — one due to Tate and Deligne, another due to Hayes. It is the author's hope that anyone who has read Chapters 14 and 15 will be inspired to go on to master one or both of the proofs of the general result.

Chapter 16 presents function field analogues of the famous class number formulas of Kummer for cyclotomic number fields together with variations on this theme. Once again, most of this material has been generalized considerably and the material in this chapter, which has its own interest, can also serve as the background for further study.

Finally, in Chapter 17 we discuss average value theorems in global fields. The material presented here generalizes work of Carlitz over the ring $A = \mathbb{F}[T]$. A novel feature is a function field analogue of the Wiener-Ikehara Tauberian theorem. The beginning of the chapter discusses average values of elementary number-theoretic functions. The last part of the chapter deals with average values for class numbers of hyperelliptic function fields.

In the effort to keep this book reasonably short, many topics which could have been included were left out. For example, chapters had been contemplated on automorphisms and the inverse Galois problem, the number of rational points with applications to algebraic coding theory, and the theory of character sums. Thought had been given to a more extensive discussion of Drinfeld modules and the subject of explicit class field theory in global fields. Also omitted is any discussion of the fascinating subject of transcendental numbers in the function field context (for an excellent survey see J. Yu [1]). Clearly, number theory in function fields is a vast subject. It is of interest for its own sake and because it has so often served as a stimulus to research in algebraic number theory and arithmetic geometry. We hope this book will arouse in the reader a desire to learn more and explore further.

I would like to thank my friends David Goss and David Hayes for their encouragement over the years and for their work which has been a constant source of delight and inspiration.

I also want to thank Allison Pacelli and Michael Reid who read several chapters and made valuable suggestions. I especially want to thank Amir Jafari and Hua-Chieh Li who read most of the book and did a thorough job spotting misprints and inaccuracies. For those that remain I accept full responsibility.

This book had its origins in a set of seven lectures I delivered at KAIST (Korean Advanced Institute of Science and Technology) in the summer of 1994. They were published in: "Lecture Notes of the Ninth KAIST Mathematics Workshop, Volume 1, 1994, Taejon, Korea." For this wonderful opportunity to bring my thoughts together on these topics I wish to thank both the Institute and my hosts, Professors S.H. Bae and J. Koo.

Years ago my friend Ken Ireland suggested the idea of writing a book together on the subject of arithmetic in function fields. His premature death in 1991 prevented this collaboration from ever taking place. This book would have been much better had we been able to do it together. His spirit and great love of mathematics still exert a deep influence over me. I hope something of this shows through on the pages that follow.

Finally, my thanks to Polly for being there when I became discouraged and for cheering me on.

December 30, 2000   Michael Rosen
                                                     Brown University