Preface

This is a modern introduction to number theory, aimed at several different audiences: students who have little experience of university level mathematics, students who are completing an undergraduate degree in mathematics, as well as students who are completing a mathematics teaching qualification. Like most introductions to number theory, our contents are largely inspired by Gauss's *Disquisitiones Arithmeticae* (1801), though we also include many modern developments. We have gone back to Gauss to borrow several excellent examples to highlight the theory.

There are many different topics that might be included in an introductory course in number theory, and others, like the law of quadratic reciprocity, that surely must appear in any such course. The first dozen chapters of the book therefore present a "standard" course. In the *masterclass* version of this book we flesh out these topics, in copious appendices, as well as adding five additional chapters on more advanced themes. In the *introductory* version we select an appendix for each chapter that might be most useful as supplementary material.[1] A "minimal" course might focus on the first eight chapters and at least one of chapters 9 and 10.[2]

Much of modern mathematics germinated from number-theoretic seed and one of our goals is to help the student appreciate the connection between the relatively simply defined concepts in number theory and their more abstract generalizations in other courses. For example, our appendices allow us to highlight how modern algebra stems from investigations into number theory and therefore serve as an introduction to algebra (including rings, modules, ideals, Galois theory, p-adic numbers,...). These appendices can be given as additional reading, perhaps as student projects, and we point the reader to further references.

Following Gauss, we often develop examples *before* giving a formal definition and a theorem, firstly to see how the concept arises naturally, secondly to conjecture a theorem that describes an evident pattern, and thirdly to see how a proof of the theorem emerges from understanding some non-trivial examples.

[1] In the main text we occasionally refer to appendices that only appear in the *masterclass* version.
[2] Several sections might be discarded; their headings are in ***bold italics.***

Why study number theory? Questions arise when studying any subject, sometimes fascinating questions that may be difficult to answer precisely. Number theory is the study of the most basic properties of the integers, literally taking integers apart to see how they are built, and there we find an internal beauty and coherence that encourages many of us to seek to understand more. Facts are often revealed by calculations, and then researchers seek proofs. Sometimes the proofs themselves, even more than the theorems they prove, have an elegance that is beguiling and reveal that there is so much more to understand. With good reason, Gauss called number theory the "*Queen of Mathematics*", ever mysterious, but nonetheless graciously sharing with those that find themselves interested. In this first course there is much that is accessible, while at the same time natural, easily framed, questions arise which remain open, stumping the brightest minds.

Once celebrated as one of the more abstract subjects in mathematics, today there are scores of applications of number theory in the real world, particularly to the theory and practice of computer algorithms. Best known is the use of number theory in designing cryptographic protocols (as discussed in chapter 10), hiding our secrets behind the seeming difficulty of factoring large numbers which only have large prime factors.

For some students, studying number theory is a life-changing experience: They find themselves excited to go on to penetrate more deeply, or perhaps to pursue some of the fascinating applications of the subject.

Why give proofs? We give proofs to convince ourselves and others that our reasoning is correct. Starting from agreed upon truths, we try to derive a further truth, being explicit and precise about each step of our reasoning. A proof must be readable by people besides the author. It is a way of communicating ideas and needs to be persuasive, not just to the writer but also to a mathematically literate person who cannot obtain further clarification from the writer on any point that is unclear. It is not enough that the writer believes it; it must be clear to others. The burden of proof lies with the author.

The word "proof" can mean different things in different disciplines. In some disciplines a "proof" can be several different examples that justify a stated hypothesis, but this is inadequate in mathematics: One can have a thousand examples that work as predicted by the hypothesis, but the thousand and first might contradict it. Therefore to "prove" a theorem, one must build an incontrovertible argument up from first principles, so that the statement must be true in every case, assuming that those first principles are true.

Occasionally we give more than one proof of an important theorem, to highlight how inevitably the subject develops, as well as to give the instructor different options for how to present the material. (Few students will benefit from seeing *all* of the proofs on their first time encountering this material.)

Motivation. Challenging mathematics courses, such as point-set topology, algebraic topology, measure theory, differential geometry, and so on, tend to be dominated at first by formal language and requirements. Little is given by way of motivation. Sometimes these courses are presented as a prerequisite for topics that will come later. There is little or no attempt to explain what all this theory is good

for or why it was developed in the first place. Students are expected to subject themselves to the course, motivated primarily by trust.

How boring! Mathematics surely should not be developed only for those few who already know that they wish to specialize and have a high tolerance for boredom. We should help our students to appreciate and cherish the beauty of mathematics. Surely courses should be motivated by a series of interesting questions. The right questions will highlight the benefits of an abstract framework, so that the student will wish to explore even the most rarified paths herself, as the benefits become obvious. Number theory does not require much in the way of formal prerequisites, and there are easy ways to justify most of its abstraction.

In this book, we hope to capture the attention and enthusiasm of the reader with the right questions, guiding her as she embarks for the first time on this fascinating journey.

Student expectations. For some students, number theory is their first course that formulates abstract statements of theorems, which can take them outside of their "comfort zone". This can be quite a challenge, especially as high school pedagogy moves increasingly to training students to learn and use sophisticated techniques, rather than appreciate how those techniques arose. We believe that one can best use (and adapt) methods if one fully appreciates their genesis, so we make no apologies for this feature of the elementary number theory course. However this means that some students will be forced to adjust their personal expectations. Future teachers sometimes ask why they need to learn material, and take a perspective, so far beyond what they will be expected to teach in high school. There are many answers to this question; one is that, in the long term, the material in high school will be more fulfilling if one can see its long-term purpose. A second response is that every teacher will be confronted by students who are bored with their high school course and desperately seeking harder intellectual challenges (whether they realize it themselves or not); the first few chapters of this book should provide the kind of intellectual stimulation those students need.

Exercises. Throughout the book, there are a lot of problems to be solved. Easy questions, moderate questions, hard questions, exceptionally difficult questions. No one should do them all. The idea of having so many problems is to give the teacher options that are suitable for the students' backgrounds:

An unusual feature of the book is that exercises appear embedded in the text.[3] This is done to enable the student to complete the proofs of theorems as one goes along.[4] This does not require the students to come up with new ideas but rather to follow the arguments given so as to fill in the gaps. For less experienced students it helps to write out the solutions to these exercises; more experienced students might just satisfy themselves that they can provide an appropriate proof.

[3]Though they can be downloaded, as a separate list, from `www.ams.org/granville-number-theory`.

[4]Often students have little experience with proofs and struggle with the level of sophistication required, at least without adequate guidance.

Other questions work through examples. There are more challenging exercises throughout, indicated by the symbol † next to the question numbers, in which the student will need to independently bring together several of the ideas that have been discussed. Then there are some really tough questions, indicated by the symbol ‡, in which the student will need to be creative, perhaps even providing ideas not given, or hinted at, in the text.

A few questions in this book are open-ended, some even phrased a little misleadingly. The student who tries to develop those themes her- or himself, might embark upon a rewarding voyage of discovery. Once, after I had set the exercises in section 9.2 for homework, some students complained how unfair they felt these questions were but were silenced by another student who announced that it was so much fun for him to work out the answers that he now knew what he wanted to do with his life!

At the end of the book we give hints for many of the exercises, especially those that form part of a proof.

Special features of our syllabus. Number theory sometimes serves as an introduction to "proof techniques". We give many exercises to practice those techniques, but to make it less boring, we do so while developing certain themes as the book progresses, for examples, the theory of recurrence sequences, and properties of binomial coefficients. We dedicate a preliminary chapter to induction and use it to develop the theory of sums of powers. Here is a list of the main supplementary themes which appear in the book:

Special numbers: Bernoulli numbers; binomial coefficients and Pascal's triangle; Fermat and Mersenne numbers; and the Fibonacci sequence and general second-order linear recurrences.

Subjects in their own right: Algebraic numbers, integers, and units; computation and running times: Continued fractions; dynamics; groups, especially of matrices; factoring methods and primality testing; ideals; irrationals and transcendentals; and rings and fields.

Formulas for cyclotomic polynomials, Dirichlet L-functions, the Riemann zeta-function, and sums of powers of integers.

Interesting issues: Lifting solutions; polynomial properties; resultants and discriminants; roots of polynomials, constructibility and pre-Galois theory; square roots (mod n); and tests for divisibility.

Fun and famous problems like the *abc*-conjecture, Catalan's conjecture, Egyptian fractions, Fermat's Last Theorem, the Frobenius postage stamp problem, magic squares, primes in arithmetic progressions, tiling with rectangles and with circles.

Our most unconventional choice is to give a version of Rousseau's proof of the law of quadratic reciprocity, which is directly motivated by Gauss's proof of Wilson's Theorem. This proof avoids Gauss's Lemma so is a lot easier for a beginning student than Eisenstein's elegant proof (which we give in section 8.10 of appendix 8A). Gauss's original proof of quadratic reciprocity is more motivated by the introductory material, although a bit more complicated than these other two proofs.

We include Gauss's original proof in section 8.14 of appendix 8C, and we also understand $(2/n)$ in his way, in the basic course, to interest the reader. We present several other proofs, including a particularly elegant proof using Gauss sums in section 14.7.

Further exploration of number theory. There is a tremendous leap in the level of mathematical knowledge required to take graduate courses in number theory, because curricula expect the student to have taken (and appreciated) several other relevant courses. This is a shame since there is so much beautiful advanced material that is easily accessible after finishing an introductory course. Moreover, it can be easier to study other courses, if one already understands their importance, rather than taking it on trust. Thus this book, *Number Theory Revealed*, is designed to lead to two subsequent books, which develop the two main thrusts of number theory research:

In *The distribution of primes: Analytic number theory revealed*, we will discuss how number theorists have sought to develop the themes of chapter 5 (as well as chapters 4 and 13). In particular we prove the prime number theorem, based on the extraordinary ideas of Riemann. This proof rests heavily on certain ideas from complex analysis, which we will outline in a way that is relevant for a good understanding of the proofs.

In *Rational points on curves: Arithmetic geometry revealed*, we look at solutions to Diophantine equations, especially those of degree two and three, extending the ideas of chapter 12 (as well as chapters 14 and 17). In particular we will prove Mordell's Theorem (developed here in special cases in chapter 17) and gain a basic understanding of modular forms, outlining some of the main steps in Wiles's proof of Fermat's Last Theorem. We avoid a deep understanding of algebraic geometry, instead proceeding by more elementary techniques and a little complex analysis (which we explain).

References. There is a list of great number theory books at the end of our book and references that are recommended for further reading at the end of many chapters and appendices. Unlike most textbooks, I have chosen to not include a reference to every result stated, nor necessarily to most relevant articles, but rather focus on a smaller number that might be accessible to the reader. Moreover, many readers are used to searching online for keywords; this works well for many themes in mathematics.[5] However the student researching online should be warned that Wikipedia articles are often out of date, sometimes misleading, and too often poorly written. It is best to try to find relevant articles published in expository research journals, such as the *American Mathematical Monthly*,[6] or posted at arxiv.org which is "open access", to supplement the course material.

The cover (designed by Marci Babineau and the author)**.**

In 1675, Isaac Newton explained his extraordinary breakthroughs in physics and mathematics by claiming, "*If I have seen further it is by standing on the shoulders*

[5]Though getting just the phrasing to find the right level of article can be challenging.

[6]Although this is behind a paywall, it can be accessed, like many journals, by logging on from most universities, which have paid subscriptions for their students and faculty.

of Giants." Science has always developed this way, no more so than in the theory of numbers. Our cover represents five giants of number theory, in a fan of cards, each of whose work built upon the previous luminaries.

Modern number theory was born from PIERRE DE FERMAT's readings of the ancient Greek texts (as discussed in section 6.1) in the mid-17th century, and his enunciation of various results including his tantalizingly difficult to prove "Last Theorem." His "Little Theorem" (chapter 7) and his understanding of sums of two squares (chapter 9) are part of the basis of the subject.

The first modern number theory book, Gauss's *Disquisitiones Arithmeticae*, on which this book is based, was written by CARL FRIEDRICH GAUSS at the beginning of the 19th century. As a teenager, Gauss rethought many of the key ideas in number theory, especially the law of quadratic reciprocity (chapter 8) and the theory of binary quadratic forms (chapter 12), as well as inspiring our understanding of the distribution of primes (chapter 5).

Gauss's contemporary SOPHIE GERMAIN made perhaps the first great effort to attack Fermat's Last Theorem (her effort is discussed in appendix 7F). Developing her work inspired my own first research efforts.

SRINIVASA RAMANUJAN, born in poverty in India at the end of the 19th century, was the most talented untrained mathematician in history, producing some extraordinary results before dying at the age of 32. He was unable to satisfactorily explain many of his extraordinary insights which penetrated difficult subjects far beyond the more conventional approaches. (See appendix 12F and chapters 13, 15, and 17.) Some of his identities are still inspiring major developments today in both mathematics and physics.

ANDREW WILES sits atop our deck. His 1994 proof of Fermat's Last Theorem built on the ideas of the previous four mentioned mathematicians and very many other "giants" besides. His great achievement is a testament to the success of science building on solid grounds.

Thanks. I would like to thank the many inspiring mathematicians who have helped me shape my view of elementary number theory, most particularly Bela Bollobas, Paul Erdős, D. H. Lehmer, James Maynard, Ken Ono, Paulo Ribenboim, Carl Pomerance, John Selfridge, Dan Shanks, and Hugh C. Williams as well as those people who have participated in developing the relatively new subject of "additive combinatorics" (see sections 15.3, 15.4, 15.5, and 15.6). Several people have shared insights or new works that have made their way into this book: Stephanie Chan, Leo Goldmakher, Richard Hill, Alex Kontorovich, Jennifer Park, and Richard Pinch. The six anonymous reviewers added some missing perspectives and Olga Balkanova, Stephanie Chan, Patrick Da Silva, Tristan Freiberg, Ben Green, Mariah Hamel, Jorge Jimenez, Nikoleta Kalaydzhieva, Dimitris Koukoulopoulos, Youness Lamzouri, Jennifer Park, Sam Porritt, Ethan Smith, Anitha Srinivasan, Paul Voutier, and Max Wenqiang Xu kindly read subsections of the near-final draft, making valuable comments.