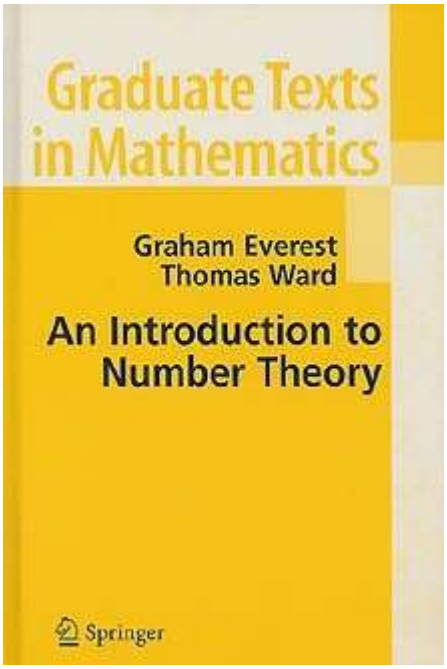
An Introduction to Number Theory by Graham Everest and Thomas Ward

Reviewed by Rob Benedetto



A former student with a BA in mathematics fresh under his belt recently asked me if I could recommend any good introductory texts on number theory. I pondered; there are so many choices! The standard undergraduate texts develop the primes in the integers, modular arithmetic, Fermat's Little Theorem, the Euler phi-function, Pythagorean triples, perfect numbers, quadratic reciprocity, and a handful of other assorted topics, all while assuming few prerequisites other than some mathematical enthusiasm. A related class of texts also starts from nearly zero (or maybe from some basic group theory) but delves deep into a single specific topic, such as elliptic curves or class groups. More advanced texts assume the reader is very well versed in analysis, allowing a quick and rigorous march through the delicate sums and integrals of analytic number theory. Still others assume a similar level of expertise in algebra, along with not a little analysis, to construct the edifice of algebraic number theory. All of these classes have wonderful representatives, and I mentioned one or two of each to the aforementioned student. Then I was handed Everest and Ward's book, which did not quite fit into any of the above categories, and I realized that it was perhaps just what the fellow was looking for.

In *An Introduction to Number Theory*, the authors strive to have the best of all worlds: they cover a broad range of topics, but they aim for some real depth in each. In particular, they discuss roughly four different "streams" of number theory: standard undergraduate number theory (including modular arithmetic and quadratic reciprocity, along with a small dose of basic algebraic number theory), Diophantine geometry, analytic number theory, and a little computational number theory. As advertised in the introduction, they provide multiple proofs for major theorems like the infinitude of primes and the analytic continuation of the zeta function. (Curiously, however, quadratic reciprocity is given only one proof). The exposition develops concepts carefully, with plenty of intuition and historical context provided, but also with full rigor. Of course, occasional steps are left to the reader, but always explicitly so. Similarly, some deeper theorems less central to the main narrative are stated without proof, but with ample references both to original papers and to expository sources. In fact, one of the great features of the book is the set of notes at the end of each chapter carefully explaining where to find more information on virtually every topic discussed. Several rarely transcribed but well-known results also appear: an off-the-beaten-path proof of the analytic continuation of zeta, short and elementary (albeit ad hoc) proofs of the infinitude of primes congruent to 1 mod 4 and to 3 mod 4, and the impossibility of a

Q-rational torsion point of order 11 on an elliptic curve, for example. In addition, many wonderful exercises are sprinkled throughout the text. A number of the exercises, marked with asterisks, are *very* hard; as the authors make clear in the introduction, they are intended as research projects, forcing most mortal readers to dig up the original papers in the library.

The book begins with the infinitude of the primes, proven in a number of (standard) ways. That provides an avenue to move quickly to Mersenne and Fermat numbers, Zsigmondy's Theorem, and primality testing. Tastes of more advanced topics, like the Riemann zeta function, are tossed in right from the start. Next come Diophantine equations, with an emphasis on sums of squares, leading into Euclidean and non-Euclidean rings (especially for rings of integers of quadratic number fields), unique factorization, class numbers and ideal class groups, quadratic reciprocity, units in real quadratic fields, and quadratic forms.

The authors then introduce elliptic curves, with a particular emphasis on the congruent number problem. They consider the subject both from the standpoint of Diophantine equations (especially rank and torsion) and from that of lattices and elliptic functions. They then introduce arithmetic heights, which they use to prove (most of) Mordell's theorem (that the group of **Q**-rational points is finitely generated). From heights, they briefly turn to canonical heights and Mahler measure; then, it's on to analytic number theory.

After some groundwork like Stirling's formula, the authors discuss arithmetic functions, Dirichlet convolution, and Möbius inversion (finally proving Zsigmondy's Theorem on Mersenne numbers in the process). Next come Euler products for multiplicative arithmetic functions, followed by a detailed discussion of the analytic continuation of the zeta function. After presenting some basic Fourier analysis and an introduction to the Gamma function, the authors prove the functional equation of the zeta function. Armed with these analytic techniques, they then make quick work of Dirichlet characters (the use of which is motivated beautifully) and their associated L-functions, leading to the infinitude of primes in arithmetic progressions. In the penultimate chapter, the authors tie much of the earlier material together in stating and proving the class number formula for quadratic fields and in introducing the Birch and Swinnerton-Dyer conjecture. Finally, the last chapter is devoted to computational number theory, including RSA, computation time, primality testing algorithms, and factorization algorithms. Although most of this chapter fits more appropriately with the first two or three chapters, there are a handful of uses of elliptic curves or L-functions that warrant its placement at the end.

The authors assume that their audience has taken some undergraduate analysis (especially complex analysis) and undergraduate algebra, but they are also very willing to accept that a reader may be rather rusty on some of the details. For example, Euler's analytic proof of the infinitude of primes appears in the first few pages; but the authors are happy to remind the reader of some basic facts about the harmonic series and the integral test along the way. Similarly, the analytic continuation of the zeta function (again, with multiple proofs) and the functional equation are proven in all their glory, and the reader is expected to have seen Cauchy's integral formula, but more than a few pages are devoted to recalling uniform convergence and its consequences. Algebra is treated in a similar fashion; when group theory would be useful in a theorem, the authors present a second proof that doesn't use it, if possible. Likewise, they assume the reader has seen rings and ideals, but they lay virtually all of it out from the definitions just in case. Of course, a student who has never before seen ring theory or uniform convergence would be steamrollered by the speed at which those topics are reviewed; but the pace seems just right for someone who has seen them before but may not have fully internalized them.

This book could be used for a number of different courses. For example, after the first chapter has been covered, the chapters on analytic number theory can stand independently of the rest of the book. Alternately, a course covering the first few chapters (up to roughly the elliptic curves chapter, with perhaps a brief tour of the final computational chapter) makes a solid and fairly traditional

undergraduate number theory course, especially if the students have taken abstract algebra and have the wherewithal to dig up some of the bibliographic sources the book points them towards. The full book would be appropriate for a first-year graduate course. It's also a nice introduction to the subject for established mathematicians from other fields. In fact, with the caveat that the book only goes so deep (no algebraic number theory beyond quadratic fields, and only the barest basics on elliptic curves, for example), its extensive bibliography, tasteful collection of topics, and clear presentation make it a pleasant reference even for working number theorists.

Publication Data: An Introduction to Number Theory, by Graham Everest and Thomas Ward. Graduate Texts in Mathematics 232, Springer-Verlag, 2005. Hardcover, x + 302 pp. $59.95. ISBN 1-85233-917-9.

Rob Benedetto is an Assistant Professor of Mathematics at Amherst College.