
MR2135478 (Review) 11-01 11-02

Everest, Graham (4-EANG)**; Ward, Thomas** (4-EANG)

★**An introduction to number theory.**

Graduate Texts in Mathematics, 232.
Springer-Verlag London, Ltd., London, 2005. x+294 *pp.* $59.95.
ISBN 978-1-85233-917-3; 1-85233-917-9

This number theory text is somewhat different than traditional number theory texts. The authors' guiding principle is unique factorization and its consequences. The first chapter discusses divisibility and primes in the context of the natural numbers and this leads to the unique factorization of the natural numbers.

The second chapter on Diophantine equations begins to open up the context in which to place unique factorization. The authors bring up Euclidean rings and mention that Euclidean rings are always unique factorization domains by virtually the same proof as for the natural numbers. An easy example of this is the Gaussian integers and the authors use this fact to discuss the sum of two squares problem as well as a few other Diophantine equations.

The third chapter generalizes Pythagorean triples, which brings in quadratic reciprocity and leads to a discussion of quadratic rings and whether or not they have unique factorization.

To recover unique factorization for those quadratic rings without it the fourth chapter discusses the theory of ideals. This concept was one of the early triumphs of algebraic number theory.

The discussion next turns to elliptic curves, which are discussed in the next three chapters. These are followed by three chapters on analytic number theory (the Riemann zeta function, its functional equation and primes in arithmetic progressions.)

In chapter eleven the authors attempt to reunite what may seem to be a somewhat disparate collection of topics. They do this by discussing the class number formula from ideal theory and the Birch and Swinnerton-Dyer conjectures. The common thread here is the L-function and the basis for much of modern number theory is related to the study of L-functions.

In the last chapter the authors show how these many number theoretic concepts can be applied to the problems of primality testing and cryptography.

This is not a traditional number theory text, but one that tries to guide the reader through the beginnings of the subject toward the modern frontiers. This is helped along by a good sized bibliography plus many problems scattered throughout the text that help in complementing the material and often are main results themselves (for

example, the Lucas-Lehmer test is an early exercise).

While this may not be a text for an undergraduate course in number theory it might provide an interesting experience when used at the graduate level. *Don Redmond* (1-SIL)