Introduction

Note. Graham Everest and Thomas Ward' *An Introduction to Number Theory*, Graduate Texts in Mathematics #232, NY: Springer (2005) assumes a background in complex analysis at the level of ETSU's Complex Variables (MATH 4337/5337), and a background in modern algebra at the level of ETSU's Introduction to Modern Algebra (MATH 4127/5127), and Introduction to Modern Algebra 2 (MATH 4137/5137). The book takes the view that complex function theory was influenced by the Fundamental Theorem of Arithmetic and the idea of factoring functions other than polynomials (such as given in Weierstrass Factorization Theorem and the Hadamard Factorization Theorem; see my online notes for Complex Analysis 2, particularly Section VII.5. The Weierstrass Factorization Theorem and Section XI.3. Hadamard's Factorization Theorem).

Note. The authors base the book on three courses they taught at the University of East Anglia "at the final-year undergraduate level." Their courses focused on (1) analytic number theory (Chapters 1, 8, 9, and 10), (2) algebraic and geometric number theory (Chapters 1, 2, 3, and 4), and (3) computational number theory (with emphasis on Chapter 1 and 12). A course on Diophantine equations or elliptic curves could cover Chapters 1, 2, 5, 6, and 7. The book starts at an elementary level; we *do* assume somewhat of a familiarity in number theory such as covered in some of the material of Mathematical Reasoning (MATH 3000; notice the Chapter 6 material) or Elementary Number Theory (MATH 3120). Though we cover some elementary material, the book is still appropriate for a graduate-level class (as evidenced by the fact that it appears in Springer-Verlag's "Graduate Texts in Mathematics" series (as volume 232).

Note. Notationally, we consider the following sets:

- The natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- The prime numbers $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$.
- The integers numbers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- The rational numbers $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$.
- The real numbers $\mathbb{R}$.
- The complex numbers $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$.

The real numbers are formally defined in Analysis 1 (MATH 4217/5217) as a complete ordered field (see Section 1.3. The Completeness Axiom). The natural numbers are axiomatically developed in a set theory class; ETSU does not have a formal set theory class, but I have online notes for Introduction to Set Theory (notice Chapter 3 on the natural numbers). The prime numbers, integers, and rational numbers can then be developed from the natural numbers algebraically.

Note. We denote a finite field with $q = p^r$ elements, where $p \in \mathbb{P}$ and $r \in \mathbb{N}$, as $\mathbb{F}_q$. Finite fields are classified in Introduction to Modern Algebra 2 (MATH 4137/5137) in Section VI. Finite Fields (see "Theorem. Structure of Finite Fields"). For field $\mathbb{F}_q$, we denote the multiplicative group of nonzero elements of $\mathbb{F}_q$ as $\mathbb{F}_q^*$. For $p \in \mathbb{F}$, $\mathbb{F}_p$ denotes the field $\{0, 1, 2, \ldots, p - 1\}$ under addition and multiplication modulo p.

Note. For $z = a + ib \in \mathbb{C}$, the book denotes the real part of z as $a = \Re(z)$ and the imaginary part as $b = \Im(z)$, but in these notes we use the more traditional notation $a = \mathrm{Re}(z)$ and $b = \mathrm{Im}(z)$. For $a, b \in \mathbb{Z}$, if $ak = b$ for some $k \in \mathbb{Z}$ then a *divides* b which we denote $a \mid b$. We denote the *cardinality* of set X as $|X|$ (as opposed to the commonly used number theory notation $\#X$). The greatest common divisor of a and b is denoted $\gcd(a, b)$ (as opposed to the common number theory notation (a, b)). We indicate multiplication with a single dot, $\cdot$.

Note. For functions f and g mapping $\mathbb{N} \to \mathbb{R}$, we consider the following *rates of growth*:

- $f \sim g$ means $\displaystyle\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$,
- $f = O(g)$ means there is a constant $A > 0$ such that $f(x) \leq Ag(x)$ for all x, and
- $f = o(g)$ means $\displaystyle\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Notice that $f = O(1)$ means that f is bounded. We denote $f = O(g)$ (which we read "f is big-Oh of g"; we read $= o(g)$ as "f is little-oh of g")) as $f \ll g$. These ideas are also introduced in Calculus 2 (MATH 1920) in Section 7.4. Relative Rates of Growth.

Revised: 4/13/2022