

1. Record Nr.	UNINA9910635397503321
Autore	McLeman Cam
Titolo	Explorations in number theory : commuting through the numbertverse / / Cam McLeman, Erin McNicholas, Colin Starr
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-030-98931-3
Descrizione fisica	1 online resource (380 pages)
Collana	Undergraduate Texts in Mathematics
Disciplina	512.74
Soggetti	Number theory Teoria de nombres Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Who is This Text's Audience? -- To the Student: -- To the Instructor: -- Suggested Pacing and Content Coverage -- Contents -- 1 What is a Number? -- 1.1 Human conception of numbers -- -- 1.2 Algebraic Number Systems -- 1.3 New Numbers, New Worlds -- 1.4 Exercises -- 2 A Quick Survey of the Last Two Millennia -- 2.1 Fermat, Wiles, and The Father of Algebra -- 2.2 Quadratic Equations -- 2.3 Diophantine Equations -- 2.4 Exercises -- 3 Number Theory in $\mathbb{Z}$ Beginning -- 3.1 Algebraic Structures -- 3.2 Linear Diophantine Equations and the Euclidean Algorithm -- 3.3 The Fundamental Theorem of Arithmetic -- 3.4 Factors and Factorials -- 3.5 The Prime Archipelago -- 3.6 Exercises -- 4 Number Theory in the Mod-n Era -- 4.1 Equivalence Relations and the Binary World -- 4.2 The Ring of Integers Modulo n -- 4.3 Reduce First and ask Questions Later -- 4.4 Division, Exponentiation, and Factorials in $\mathbb{Z}_n$ -- 4.5 Group Theory and the Ring of Integers Modulo n -- 4.6 Lagrange's Theorem and the Euler Totient Function -- 4.7 Sunzi's Remainder Theorem and $\phi(n)$ -- 4.8 Phis, Polynomials, and Primitive Roots -- 4.9 Exercises -- 5 Gaussian Number Theory: Zi of the Storm -- 5.1 The Calm Before -- 5.2 Gaussian Divisibility -- 5.3 Gaussian Modular Arithmetic -- 5.4 Gaussian Division Algorithm: The Geometry of Numbers -- 5.5 A Gausso-Euclidean Algorithm -- 5.6 Gaussian Primes and Prime

Factorizations -- 5.7 Applications to Diophantine Equations -- 5.8 Exercises -- 6 Number Theory, from Where We R to Across the C -- 6.1 From  $-1$  to  $-d$  -- 6.2 Algebraic Numbers and Rings of Integers -- 6.3 Quadratic Fields: Integers, Norms, and Units -- 6.4 Euclidean Domains -- 6.5 Unique Factorization Domains -- 6.6 Euclidean Rings of Integers -- 6.7 Exercises -- 7 Cyclotomic Number Theory: Roots and Reciprocity -- 7.1 Introduction -- 7.2 Quadratic Residues and Legendre Symbols. 7.3 Quadratic Residues and Non-Residues Mod  $p$  -- 7.4 Application: Counting Points on Curves -- 7.5 The Quadratic Reciprocity Law: Statement and Use -- 7.6 Some Unexpected Helpers: Roots of Unity -- 7.7 A Proof of Quadratic Reciprocity -- 7.8 Quadratic UFDs -- 7.9 Exercises -- 8 Number Theory Unleashed: Release  $\mathbb{Z}_p$  -- 8.1 The Analogy between Numbers and Polynomials -- 8.2 The  $p$ -adic World: An Analogy Extended -- 8.3  $p$ -adic Arithmetic: Making a Ring -- 8.4 Which numbers are  $p$ -adic? -- 8.5 Hensel's Lemma -- 8.6 The Local-Global Philosophy and the Infinite Prime -- 8.7 The Local-Global Principle for Quadratic Equations -- 8.8 Computations: Quadratic Equations Made Easy -- 8.9 Synthesis and Beyond: Moving Between Worlds -- 8.10 Exercises -- 9 The Adventure Continues -- 9.1 Exploration: Fermat's Last Theorem for Small  $n$  -- 9.2 Exploration: Lagrange's Four-Square Theorem -- 9.3 Exploration: Public Key Cryptography -- 9.3.1 Public Key Encryption: RSA -- 9.3.2 Elliptic Curve Cryptography -- 9.3.3 Elliptic ElGamal Public Key Cryptosystem -- 9.4 Exploration: Units of Real Quadratic Fields -- 9.5 Exploration: Ideals and Ideal Numbers -- 9.6 Conclusion: The Numberverse, Redux -- Appendix I Number Systems -- I.1 Introduction -- I.2 Construction of the Natural Numbers -- I.3 Induction and Well-Ordering -- Appendix Index -- Index -- Appendix Index of Notation -- Author Index.

---