
Contents

Preface	vii
Introduction	ix
Chapter 1. Three Motivating Problems	1
§1.1. Fermat's Last Theorem	3
§1.2. The Congruent Number Problem	5
§1.3. Cryptography	6
Chapter 2. Back to the Beginning	9
§2.1. The Unit Circle: Real vs. Rational Points	10
§2.2. Parametrizing the Rational Points on the Unit Circle	12
§2.3. Finding all Pythagorean Triples	16
§2.4. Looking for Underlying Structure: Geometry vs. Algebra	27
§2.5. More about Points on Curves	34
§2.6. Gathering Some Insight about Plane Curves	38
§2.7. Additional Exercises	43
Chapter 3. Some Elementary Number Theory	45
§3.1. The Integers	46
§3.2. Some Basic Properties of the Integers	47

§3.3.	Euclid's Algorithm	52
§3.4.	A First Pass at Modular Arithmetic	56
§3.5.	Elementary Cryptography: Caesar Cipher	63
§3.6.	Affine Ciphers and Linear Congruences	66
§3.7.	Systems of Congruences	70
Chapter 4.	A Second View of Modular Arithmetic: \mathbb{Z}_n and U_n	73
§4.1.	Groups and Rings	73
§4.2.	Fractions and the Notion of an Equivalence Relation	77
§4.3.	Modular Arithmetic	79
§4.4.	A Few More Comments on the Euler Totient Function	93
§4.5.	An Application to Factoring	95
Chapter 5.	Public-Key Cryptography and RSA	101
§5.1.	A Brief Overview of Cryptographic Systems	102
§5.2.	RSA	107
§5.3.	Hash Functions	114
§5.4.	Breaking Cryptosystems and Practical RSA Security Considerations	123
Chapter 6.	A Little More Algebra	127
§6.1.	Towards a Classification of Groups	128
§6.2.	Cayley Tables	128
§6.3.	A Couple of Non-abelian Groups	131
§6.4.	Cyclic Groups and Direct Products	134
§6.5.	Fundamental Theorem of Finite Abelian Groups	138
§6.6.	Primitive Roots	141
§6.7.	Diffie–Hellman Key Exchange	143
§6.8.	ElGamal Encryption	144
Chapter 7.	Curves in Affine and Projective Space	147
§7.1.	Affine and Projective Space	147
§7.2.	Curves in the Affine and Projective Plane	153

§7.3. Rational Points on Curves	156
§7.4. The Group Law for Points on an Elliptic Curve	159
§7.5. A Formula for the Group Law on an Elliptic Curve	179
§7.6. The Number of Points on an Elliptic Curve	185
Chapter 8. Applications of Elliptic Curves	189
§8.1. Elliptic Curves and Factoring	190
§8.2. Elliptic Curves and Cryptography	196
§8.3. Remarks on a Post-Quantum Cryptographic World	198
Appendix A. Deeper Results and Concluding Thoughts	203
§A.1. The Congruent Number Problem and Tunnell's Solution	203
§A.2. A Digression on Functions of a Complex Variable	209
§A.3. Return to the Birch and Swinnerton-Dyer Conjecture	211
§A.4. Elliptic Curves over \mathbb{C}	212
Appendix B. Answers to Selected Exercises	219
§B.1. Chapter 2	219
§B.2. Chapter 3	231
§B.3. Chapter 4	233
§B.4. Chapter 5	236
§B.5. Chapter 6	238
§B.6. Chapter 7	241
Bibliography	245
Index	249