

Contents

1. Finite Structures

1. Review of $\mathbf{Z}/n\mathbf{Z}$, $(\mathbf{Z}/n\mathbf{Z})^*$, \mathbf{F}_q and \mathbf{F}_q^*	1
2. The Group Structure of $(\mathbf{Z}/n\mathbf{Z})^*$ and \mathbf{F}_q^*	5
3. Jacobi and Legendre Symbols	7
4. Gauss Sums	11
5. Applications to the Number of Solutions of Equations	15
6. Exercises	23

2. Applications: Algorithms, Primality and Factorization, Codes

1. Basic Algorithms	35
2. Cryptography, RSA	38
3. Primality Test (I)	40
4. Primality Test (II)	46
5. Factorization	51
6. Error-Correcting Codes	54
6.1. Generalities about Error-Correcting Codes	54
6.2. Linear Cyclic Codes	59
7. Exercises	66

3. Algebra and Diophantine Equations

1. Sums of Squares	76
2. Fermat's Equation ($n = 3$ and 4)	81
3. Pell's Equation $x^2 - dy^2 = 1$	85
4. Rings of Algebraic Integers	95
5. Geometry of Numbers	105
6. Exercises	113

4. Analytic Number Theory

1. Elementary Statements and Estimates	125
2. Holomorphic Functions (Summary/Reminders)	131

3. Dirichlet Series and the Function $\zeta(s)$	135
4. Characters and Dirichlet's Theorem	139
5. The Prime Number Theorem	148
6. Exercises	158
5. Elliptic Curves	
1. Group Law on a Cubic	169
2. Heights	174
2.1. Weil Heights	174
2.2. Néron-Tate Heights	183
3. The Mordell-Weil Theorem	185
4. Siegel's Theorem	189
5. Elliptic Curves over the Complex Numbers	192
6. Elliptic Curves over a Finite Field	197
7. The L -function of an Elliptic Curve	199
6. Developments and Open Problems	
1. The Number of Solutions of Equations over Finite Fields . . .	206
2. Diophantine Equations and Algebraic Geometry	212
3. p -adic Numbers	221
4. Transcendental Numbers and Diophantine Approximation . .	229
5. The a, b, c Conjecture	240
6. Some Remarkable Dirichlet Series	247
A. Factorization	
1. Polynomial Factorization	259
2. Factorization and Elliptic Curves	262
3. Factorization and Number Fields	265
B. Elementary Projective Geometry	
1. Projective Space	271
2. Intersection	279
C. Galois Theory	
1. Galois Theory and Number Fields	285
2. Abelian Extensions	289
3. Galois Representations	293
Bibliography	297
List of Notations	303
Index	307

Arithmetics

Hindry, M.

2011, XVIII, 322 p. 5 illus., Softcover

ISBN: 978-1-4471-2130-5