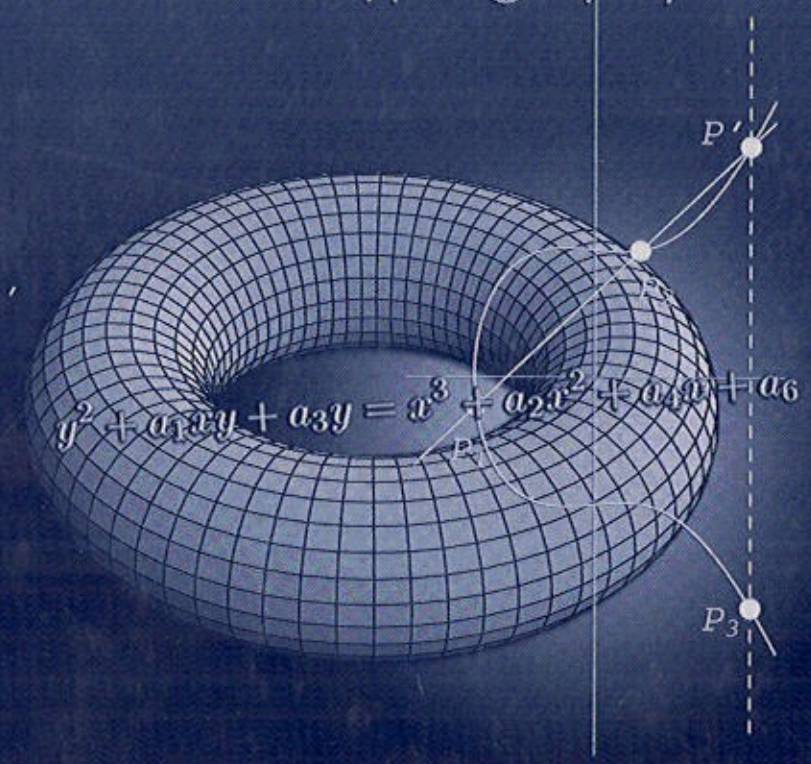
DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

# ELLIPTIC CURVES

## Number Theory and Cryptography




Lawrence C. Washington

CHAPMAN & HALL/CRC

# *Contents*


**1 Introduction** 1
Exercises . . . 8

**2 The Basic Theory** 9
2.1 Weierstrass Equations . . . 9
2.2 The Group Law . . . 12
2.3 Projective Space and the Point at Infinity . . . 18
2.4 Proof of Associativity . . . 20
2.4.1 The Theorems of Pappus and Pascal . . . 32
2.5 Other Equations for Elliptic Curves . . . 35
2.5.1 Legendre Equation . . . 35
2.5.2 Cubic Equations . . . 35
2.5.3 Quartic Equations . . . 36
2.5.4 Intersection of Two Quadratic Surfaces . . . 39
2.6 The j-invariant . . . 41
2.7 Elliptic Curves in Characteristic 2 . . . 44
2.8 Endomorphisms . . . 46
2.9 Singular Curves . . . 55
2.10 Elliptic Curves mod n . . . 59
Exercises . . . 67

**3 Torsion Points** 73
3.1 Torsion Points . . . 73
3.2 Division Polynomials . . . 76
3.3 The Weil Pairing . . . 82
Exercises . . . 86

**4 Elliptic Curves over Finite Fields** 89
4.1 Examples . . . 89
4.2 The Frobenius Endomorphism . . . 92
4.3 Determining the Group Order . . . 96
4.3.1 Subfield Curves . . . 96
4.3.2 Legendre Symbols . . . 98
4.3.3 Orders of Points . . . 100
4.3.4 Baby Step, Giant Step . . . 103
4.4 A Family of Curves . . . 105
4.5 Schoof's Algorithm . . . 113

4.6 Supersingular Curves . . . . . 120
Exercises . . . . . 130

**5 The Discrete Logarithm Problem** **133**
5.1 The Index Calculus . . . . . 134
5.2 General Attacks on Discrete Logs . . . . . 136
5.2.1 Baby Step, Giant Step . . . . . 136
5.2.2 Pollard's $\rho$ and $\lambda$ Methods . . . . . 137
5.2.3 The Pohlig-Hellman Method . . . . . 141
5.3 The MOV Attack . . . . . 144
5.4 Anomalous Curves . . . . . 147
5.5 The Tate-Lichtenbaum Pairing . . . . . 153
5.6 Other Attacks . . . . . 156
Exercises . . . . . 156

**6 Elliptic Curve Cryptography** **159**
6.1 The Basic Setup . . . . . 159
6.2 Diffie-Hellman Key Exchange . . . . . 160
6.3 Massey-Omura Encryption . . . . . 163
6.4 ElGamal Public Key Encryption . . . . . 164
6.5 ElGamal Digital Signatures . . . . . 165
6.6 The Digital Signature Algorithm . . . . . 168
6.7 A Public Key Scheme Based on Factoring . . . . . 169
6.8 A Cryptosystem Based on the Weil Pairing . . . . . 173
Exercises . . . . . 175

**7 Other Applications** **179**
7.1 Factoring Using Elliptic Curves . . . . . 179
7.2 Primality Testing . . . . . 184
Exercises . . . . . 187

**8 Elliptic Curves over Q** **189**
8.1 The Torsion Subgroup. The Lutz-Nagell Theorem . . . . . 189
8.2 Descent and the Weak Mordell-Weil Theorem . . . . . 198
8.3 Heights and the Mordell-Weil Theorem . . . . . 206
8.4 Examples . . . . . 214
8.5 The Height Pairing . . . . . 221
8.6 Fermat's Infinite Descent . . . . . 222
8.7 2-Selmer Groups; Shafarevich-Tate Groups . . . . . 227
8.8 A Nontrivial Shafarevich-Tate Group . . . . . 229
8.9 Galois Cohomology . . . . . 234
Exercises . . . . . 244

**9 Elliptic Curves over C** **247**
9.1 Doubly Periodic Functions . . . . . 247
9.2 Tori are Elliptic Curves . . . . . 257
9.3 Elliptic Curves over C . . . . . 262
9.4 Computing Periods . . . . . 275
9.4.1 The Arithmetic-Geometric Mean . . . . . 277
9.5 Division Polynomials . . . . . 283
Exercises . . . . . 291

**10 Complex Multiplication** **295**
10.1 Elliptic Curves over C . . . . . 295
10.2 Elliptic Curves over Finite Fields . . . . . 302
10.3 Integrality of j-invariants . . . . . 306
10.4 Numerical Examples . . . . . 314
10.5 Kronecker's Jugendtraum . . . . . 320
Exercises . . . . . 321

**11 Divisors** **323**
11.1 Definitions and Examples . . . . . 323
11.2 The Weil Pairing . . . . . 333
11.3 The Tate-Lichtenbaum Pairing . . . . . 338
11.4 Computation of the Pairings . . . . . 341
11.5 Genus One Curves and Elliptic Curves . . . . . 346
Exercises . . . . . 353

**12 Zeta Functions** **355**
12.1 Elliptic Curves over Finite Fields . . . . . 355
12.2 Elliptic Curves over Q . . . . . 359
Exercises . . . . . 368

**13 Fermat's Last Theorem** **371**
13.1 Overview . . . . . 371
13.2 Galois Representations . . . . . 374
13.3 Sketch of Ribet's Proof . . . . . 380
13.4 Sketch of Wiles's Proof . . . . . 387

**A Number Theory** **397**

**B Groups** **403**

**C Fields** **407**

**References** **415**

**Index** **425**