

ELLIPTIC CURVES

NUMBER THEORY AND CRYPTOGRAPHY

SECOND EDITION

LAWRENCE C. WASHINGTON

Like its bestselling predecessor, **Elliptic Curves: Number Theory and Cryptography, Second Edition** develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. With additional material, this edition offers more comprehensive coverage of the fundamental theory, techniques, and applications of elliptic curves.

New to the Second Edition

- Chapters on isogenies and hyperelliptic curves
- A discussion of alternative coordinate systems, such as projective, Jacobian, and Edwards coordinates, along with related computational issues
- A more complete treatment of the Weil and Tate–Lichtenbaum pairings
- Doud’s analytic method for computing torsion on elliptic curves over $\mathbb{Q}$
- An explanation of how to perform calculations with elliptic curves in several popular computer algebra systems

Taking a basic approach to elliptic curves, this accessible book prepares readers to tackle more advanced problems in the field. It introduces elliptic curves over finite fields early in the text, before moving on to interesting applications, such as cryptography, factoring, and primality testing. The book also discusses the use of elliptic curves in Fermat’s Last Theorem. Relevant abstract algebra material on group theory and fields can be found in the appendices.



CRC Press

Taylor & Francis Group
an **informa** business

www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

C7146

ISBN 1-4200-7146-7

90000



9 781420 071467

www.crcpress.com

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	33
2.5	Other Equations for Elliptic Curves	35
2.5.1	Legendre Equation	35
2.5.2	Cubic Equations	36
2.5.3	Quartic Equations	37
2.5.4	Intersection of Two Quadratic Surfaces	39
2.6	Other Coordinate Systems	42
2.6.1	Projective Coordinates	42
2.6.2	Jacobian Coordinates	43
2.6.3	Edwards Coordinates	44
2.7	The j -invariant	45
2.8	Elliptic Curves in Characteristic 2	47
2.9	Endomorphisms	50
2.10	Singular Curves	59
2.11	Elliptic Curves mod n	64
	Exercises	71
3	Torsion Points	77
3.1	Torsion Points	77
3.2	Division Polynomials	80
3.3	The Weil Pairing	86
3.4	The Tate-Lichtenbaum Pairing	90
	Exercises	92
4	Elliptic Curves over Finite Fields	95
4.1	Examples	95
4.2	The Frobenius Endomorphism	98
4.3	Determining the Group Order	102
4.3.1	Subfield Curves	102

4.3.2	Legendre Symbols	104
4.3.3	Orders of Points	106
4.3.4	Baby Step, Giant Step	112
4.4	A Family of Curves	115
4.5	Schoof's Algorithm	123
4.6	Supersingular Curves	130
	Exercises	139
5	The Discrete Logarithm Problem	143
5.1	The Index Calculus	144
5.2	General Attacks on Discrete Logs	146
5.2.1	Baby Step, Giant Step	146
5.2.2	Pollard's ρ and λ Methods	147
5.2.3	The Pohlig-Hellman Method	151
5.3	Attacks with Pairings	154
5.3.1	The MOV Attack	154
5.3.2	The Frey-Rück Attack	157
5.4	Anomalous Curves	159
5.5	Other Attacks	165
	Exercises	166
6	Elliptic Curve Cryptography	169
6.1	The Basic Setup	169
6.2	Diffie-Hellman Key Exchange	170
6.3	Massey-Omura Encryption	173
6.4	ElGamal Public Key Encryption	174
6.5	ElGamal Digital Signatures	175
6.6	The Digital Signature Algorithm	179
6.7	ECIES	180
6.8	A Public Key Scheme Based on Factoring	181
6.9	A Cryptosystem Based on the Weil Pairing	184
	Exercises	187
7	Other Applications	189
7.1	Factoring Using Elliptic Curves	189
7.2	Primality Testing	194
	Exercises	197
8	Elliptic Curves over $\mathbb{Q}$	199
8.1	The Torsion Subgroup. The Lutz-Nagell Theorem	199
8.2	Descent and the Weak Mordell-Weil Theorem	208
8.3	Heights and the Mordell-Weil Theorem	215
8.4	Examples	223
8.5	The Height Pairing	230
8.6	Fermat's Infinite Descent	231

8.7	2-Selmer Groups; Shafarevich-Tate Groups	236
8.8	A Nontrivial Shafarevich-Tate Group	239
8.9	Galois Cohomology	244
	Exercises	253
9	Elliptic Curves over $\mathbb{C}$	257
9.1	Doubly Periodic Functions	257
9.2	Tori are Elliptic Curves	267
9.3	Elliptic Curves over $\mathbb{C}$	272
9.4	Computing Periods	286
9.4.1	The Arithmetic-Geometric Mean	288
9.5	Division Polynomials	294
9.6	The Torsion Subgroup: Doud's Method	302
	Exercises	307
10	Complex Multiplication	311
10.1	Elliptic Curves over $\mathbb{C}$	311
10.2	Elliptic Curves over Finite Fields	318
10.3	Integrality of j -invariants	322
10.4	Numerical Examples	330
10.5	Kronecker's Jugendtraum	336
	Exercises	337
11	Divisors	339
11.1	Definitions and Examples	339
11.2	The Weil Pairing	349
11.3	The Tate-Lichtenbaum Pairing	354
11.4	Computation of the Pairings	358
11.5	Genus One Curves and Elliptic Curves	364
11.6	Equivalence of the Definitions of the Pairings	370
11.6.1	The Weil Pairing	371
11.6.2	The Tate-Lichtenbaum Pairing	374
11.7	Nondegeneracy of the Tate-Lichtenbaum Pairing	375
	Exercises	379
12	Isogenies	381
12.1	The Complex Theory	381
12.2	The Algebraic Theory	386
12.3	Vélu's Formulas	392
12.4	Point Counting	396
12.5	Complements	401
	Exercises	402

13 Hyperelliptic Curves	407
13.1 Basic Definitions	407
13.2 Divisors	409
13.3 Cantor's Algorithm	417
13.4 The Discrete Logarithm Problem	420
Exercises	426
14 Zeta Functions	429
14.1 Elliptic Curves over Finite Fields	429
14.2 Elliptic Curves over $\mathbb{Q}$	433
Exercises	442
15 Fermat's Last Theorem	445
15.1 Overview	445
15.2 Galois Representations	448
15.3 Sketch of Ribet's Proof	454
15.4 Sketch of Wiles's Proof	461
A Number Theory	471
B Groups	477
C Fields	481
D Computer Packages	489
D.1 Pari	489
D.2 Magma	492
D.3 SAGE	494
References	501
Index	509