

Contents

Contents

vii

I	Plane Curves	5
1	Basic definitions; Bezout's theorem	5
2	Rational points on plane curves	17
3	The group law on a cubic curve	25
4	Regular functions; the Riemann-Roch theorem	29
5	Defining algebraic curves over subfields	42
II	Basic Theory of Elliptic Curves	45
1	Definition of an elliptic curve	45
2	The Weierstrass equation for an elliptic curve	50
3	Reduction of an elliptic curve modulo p	54
4	Elliptic curves over $\mathbb{Q}_p$	61
5	Torsion points	64
6	Néron models	69
7	Algorithms for elliptic curves	76
III	Elliptic Curves over the Complex Numbers	81
1	Lattices and bases	81
2	Doubly periodic functions	82
3	Elliptic curves as Riemann surfaces	89
IV	The Arithmetic of Elliptic Curves	101
1	Group cohomology	102
2	The Selmer and Tate-Shafarevich groups	108
3	The finiteness of the Selmer group	110
4	Heights; completion of the proof	117
5	The problem of computing the rank of $E(\mathbb{Q})$	126
6	The Néron-Tate pairing	131
7	Geometric interpretation of the cohomology groups	133
8	Failure of the Hasse (local-global) principle	143
9	Elliptic curves over finite fields	147

10	The conjecture of Birch and Swinnerton-Dyer	160
11	Elliptic curves and sphere packings	168
V	Elliptic curves and modular forms	173
1	The Riemann surfaces $X_0(N)$	173
2	$X_0(N)$ as an algebraic curve over $\mathbb{Q}$	181
3	Modular forms	189
4	Modular forms and the L -series of elliptic curves	193
5	Statement of the main theorems	208
6	How to get an elliptic curve from a cusp form	210
7	Why the L -Series of E_f agrees with the L -Series of f	215
8	Wiles's proof	222
9	Fermat, at last	226
	Bibliography	229
	Index	235