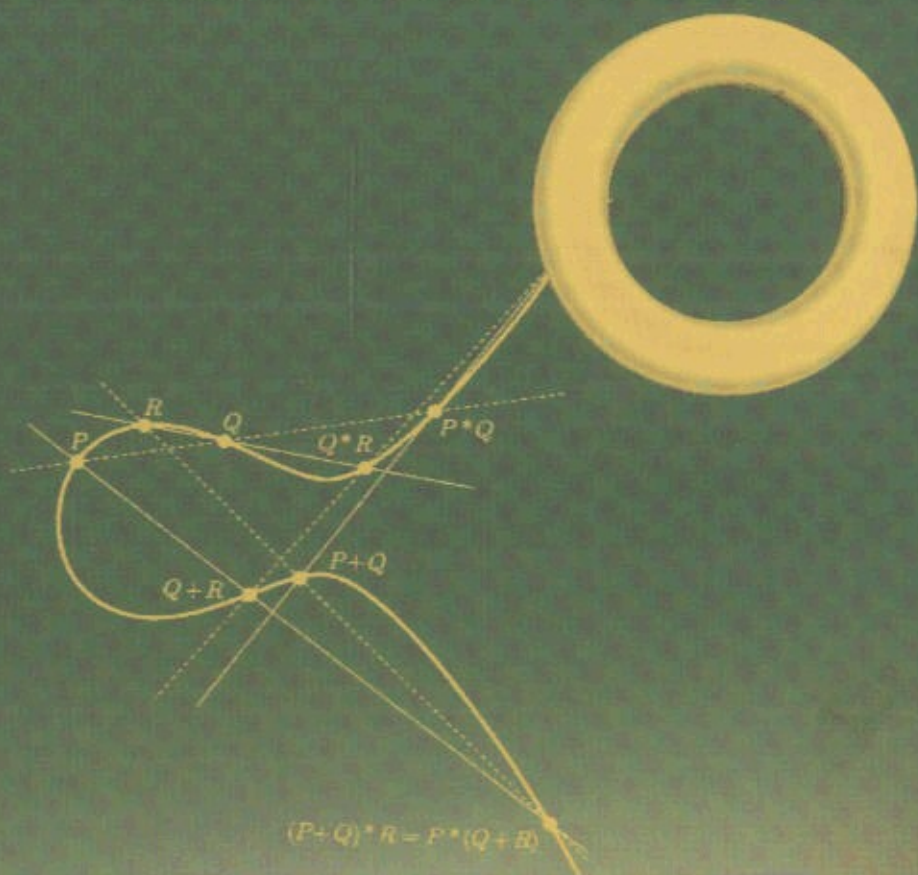


Elliptic Curves

R V Gurjar • Kirti Joshi • N Mohan Kumar • Kapil H Paranjape
A Ramanathan • T N Shorey • R R Simha • V Srinivas




Narosa



TIFR
Mumbai

Contents

Foreword	v
Preface	vii
I Analytic Theory of Elliptic Curves	1
1 Doubly Periodic Functions	3
1.1 Introduction	3
1.2 Periodic and elliptic functions	6
2 Riemann Surfaces	17
2.1 Generalities on Riemann surfaces	17
2.2 Examples	18
2.3 Holomorphic 1-forms	24
2.4 Integration of 1-forms	24
3 Tori	27
3.1 Complex tori; Embedding in $\mathbb{P}^2$	27
3.2 Addition theorem for $\wp$; the group law on cubics	30
4 Isomorphism of Tori and the j invariant	35
4.1 Isomorphism of tori	35
4.2 The functions $g_2(\tau)$, $g_3(\tau)$, $j(\tau)$	36
4.3 Isomorphism of plane cubics in terms of j	38
5 All Smooth Cubics are Complex Tori	41
5.1 The first proof	41
5.2 Second proof	48
5.3 Elliptic integrals	49

6	Moduli	53
6.1	A fundamental region for $SL(2, \mathbb{Z})$	53
6.2	Behaviour of the j function in R^0	56
6.3	The Riemann surface $\mathcal{H}/PSL(2, \mathbb{Z})$	57
6.4	Biholomorphic maps of $\mathbb{C}/\Gamma$	59
II	Algebraic Geometry of Elliptic Curves	63
7	Some Results From Commutative Algebra	65
7.1	Noetherian rings	65
7.2	Localisation	71
7.3	Integral extensions	76
7.4	Noether normalisation, and the Nullstellensatz	79
7.5	Discrete valuation rings	85
7.6	Dedekind domains	91
8	Varieties	97
8.1	Affine varieties	97
8.2	Projective varieties	107
8.3	Morphisms	112
8.4	Smooth varieties	114
9	Further Properties of Varieties	119
9.1	Product varieties	119
9.2	Completeness of projective varieties	121
9.3	Proper morphisms	124
10	Intersection Theory for Plane Curves	127
10.1	Intersection multiplicities	127
10.2	Applications of Bezout's Theorem	133
11	Geometry of Curves	141
11.1	Rational maps	141
11.2	Non-singular models	148
11.3	Group actions on curves	150
11.4	Varieties over non-algebraically closed fields	151
11.5	Divisors and linear equivalence	156

12 Geometry of Elliptic Curves	159
12.1 Riemann-Roch for elliptic curves	159
12.2 Differentials	161
12.3 The chord and tangent construction	167
12.4 Curves of genus 1	175
12.4.1 Cubic curves	177
12.4.2 Double covers	178
12.4.3 Complete intersections	180
13 Structure of Endomorphisms of Elliptic Curves	183
13.1 Endomorphisms of elliptic curves	183
13.2 The Frobenius morphism	186
13.3 Dual isogenies	190
13.4 Additivity of the invariant differential	196
13.5 The Riemann Hypothesis	198
13.6 The structure of the endomorphism ring	200
 III Arithmetic of Elliptic Curves	 203
14 Rational Points on Curves	205
14.1 Curves of degree ≤ 2	205
14.1.1 Linear equations	206
14.1.2 Equations of degree two	207
14.2 Problems of higher degree	214
14.2.1 The Fermat quartic	215
14.2.2 Frenicle's problem	218
15 The Mordell-Weil Theorem	221
15.1 The Mordell-Weil Theorem	221
15.2 Heights	230
16 Computing the Mordell-Weil Group	245
16.1 Descent	245
16.2 Local methods	247
16.3 Selmer and Tate-Shafarevich groups	255
16.4 Torsion points	257
16.4.1 Specialization modulo a prime	257

16.4.2	Mazur's theorem	264
17	The Theorems of Thue and Siegel	271
17.1	Siegel's theorem on integer points of elliptic curves . .	271
17.2	A theorem of Thue	275
17.2.1	Introduction	275
17.2.2	Two lemmas	278
17.2.3	Proof of Theorem 17.2.1	280
17.2.4	Proof of Theorem 17.2.2	281
17.2.5	Proof of Theorem 17.2.3	290
18	Representation of Numbers by Squares	293
18.1	The theta function	294
18.2	Eisenstein series	299
18.3	Cusp forms	306
19	The Conjecture of Birch and Swinnerton-Dyer	319
19.1	Introduction	319
19.2	Zeta functions over finite fields	321
19.3	Reformulating the conjecture	323
19.4	Final Form	326
IV	Appendices	331
A	Some Results From Algebraic Number Theory	333
B	The Poisson Summation Formula	337
C	Recent Developments	339
	Bibliography	343
	Index	349