

Contents

Preface	vii
1 Elliptic curves and equations	1
1.1 A general overview	1
1.2 Elliptic curves and the Mordell–Weil Theorem	5
2 Heights	9
2.1 Notations and facts	9
2.2 Absolute values in a number field	11
2.3 Heights: Absolute and logarithmic	13
2.4 A formula for the absolute logarithmic height	18
2.5 Heights of points on an elliptic curve	20
2.6 The canonical height	23
3 Weierstrass equations over $\mathbb{C}$ and $\mathbb{R}$	29
3.1 The Weierstrass $\wp$ function	29
3.2 The Weierstrass equation	31
3.3 $\psi : E(\mathbb{C}) \mapsto \mathbb{C}/\Lambda$	33
3.4 Weierstrass equations with real coefficients	36
3.4.1 $\Delta > 0$	38
3.4.2 $\Delta < 0$	40
3.4.3 Explicit expressions for the periods	41
3.4.4 Computing ω_1 and ω_2 in practice	44
3.5 $\psi : E(\mathbb{R}) \mapsto \mathbb{C}/\Lambda$ and $\iota : E(\mathbb{R}) \rightarrow \mathbb{R}/\mathbb{Z}\omega_1$	47
4 The elliptic logarithm method	54
5 Linear form for the Weierstrass equation	57
6 Linear form for the quartic equation	60
7 Linear form for simultaneous Pell equations	69

8	Linear form for the general elliptic equation	78
8.1	A short Weierstrass model	78
8.2	Puiseux series	80
8.3	Large solutions	84
8.4	The elliptic integrals	86
8.5	Computing in practice B_1 of Proposition 8.3.2	89
8.6	Computing in practice B_2 and c_9 of Proposition 8.4.2	91
8.7	The linear form $L(P)$ and its upper bound	94
9	Bound for the coefficients of the linear form	98
9.1	Lower bound for linear forms in elliptic logarithms	98
9.2	Computational remarks	105
9.3	Weierstrass equation example	107
9.4	Quartic equation example	110
9.5	Simultaneous Pell equations example	114
9.6	General elliptic equation: A quintic example	118
10	Reducing the bound obtained in Chapter 9	121
10.1	Reduction using the LLL-algorithm	122
10.2	Examples	125
10.2.1	Weierstrass equation	125
10.2.2	Quartic equation	127
10.2.3	System of simultaneous Pell equations	131
10.2.4	General elliptic equation: A quintic example	134
11	S-integer solutions of Weierstrass equations	137
11.1	The formal group of C and p -adic elliptic logarithms	137
11.2	Points with coordinates in $\mathbb{Z}_S$	144
11.3	The p -adic reduction	154
11.4	Example	158
	List of symbols	165
	Bibliography	173
	Index	177