
Contents

Preface	xiii
Part 1. Review Chapters	
Chapter 1. Rational and integer points on linear curves	15
1.1. Rational points on lines	15
1.2. Finding all the rational points on a line	16
1.3. Integer points on lines	17
1.4. Are there any integral points?	18
1.5. Finding a first integral point	18
1.6. An important reformulation	20
1.7. p -adic solutions	20
Chapter 2. Rational solutions to quadratic equations	22
2.1. Reduction to diagonal equations	22
2.2. The Pythagorean equation	23
2.3. Finding all rational points on a quadratic curve	26
2.4. Squares modulo m	28
2.5. Sums of two squares	30
2.6. Existence of solutions to quadratic equations	33
2.7. Obstructions to solutions of quadratic equations	35
2.8. The Hasse-Minkowski principle	35
2.9. Local-Global principle for higher degree	36
Chapter 3. Integer solutions to quadratic equations	37
3.1. Integer points on a given quadratic curve	37
3.2. Infinitely many solutions to Pell's equation	38

3.3. Solutions of $x^2 - dy^2 = n$ with $d > 0$	40
3.4. Finding a solution to Pell's equation	41
3.5. The Weil map and Pell's equation	44
3.6. Integral and rational points on curves: What we now know and will know	47
Chapter 4. Some descent arguments already encountered	48
4.1. Irrationality of $\sqrt{2}$	48
4.2. Fermat's "infinite descent"	49
4.3. Euler's descent for the Fermat equation with exponent 3	50
Chapter 5. Finite fields	52
5.1. Finite fields	52
5.2. Repeated roots	55
Chapter 6. Values of rational functions	56
6.1. Resultants and Discriminants	56
6.2. Growth of rational points in maps	58
6.3. Canonical height	60
6.4. Bounding ramification	61
Chapter 7. p -adic solutions	63
7.1. Lifting solutions and p -adics	63
7.2. Solutions to Diophantine equations mod p^k from solutions mod p	65
7.3. Certain special C_d	66
Part 2. Counting points on curves mod p	
Chapter 8. Counting points on linear and quadratic curves mod p , and beyond	69
8.1. Linear equations mod p	69
8.2. Quadratic equations mod p	69
8.3. A more general viewpoint, heuristically	70
8.4. A more general viewpoint. The number of solutions mod p	71
Chapter 9. Counting points on cubic curves mod p	75
9.1. The diagonal cubic equation mod $p \equiv 1 \pmod{3}$	75
9.2. The curve $E_a : y^2 = x^3 + ax$.	76
9.3. The equation $E_b : y^2 = x^3 + b$	77
9.4. The number of solutions to $y^2 \equiv f(x) \pmod{p}$	80
9.5. The number of solutions mod p , to cubic equations	81
9.6. The failure of the local-global principle for cubics	81

Part 3. The geometry of cubic curves

Chapter 10. Rational points on higher degree curves	85
10.1. Equation transformations: A brief review	85
10.2. The non-existence of parametrized solutions	86
10.3. Rational points on arbitrary cubic curve	88
10.4. Constructing new rational points on cubic curves from old ones	88
10.5. Constructing new rational points from old: A more formal perspective	90
Chapter 11. Degree three curves — why the curve $y^2 = x^3 + ax + b$?	91
11.1. Cubic curves into Weierstrass form	91
11.2. The Weierstrass form mod p	93
11.3. Diagonal cubic curves	94
11.4. y^2 equals a quartic, with a rational point	95
11.5. Two quadratic polynomials in three variables	96
Part 4. The group law; algebraic and analytic	
Chapter 12. The rational points on an elliptic curve	99
12.1. The group of rational points on an elliptic curve	99
12.2. The group law on the circle, as an elliptic curve	103
12.3. No non-trivial rational points by descent	104
12.4. The group of rational points of $y^2 = x^3 - x$	104
12.5. The height of rational points	107
Chapter 13. The Weierstrass \wp -function	109
13.1. Double periodicity and the Weierstrass \wp -function	109
13.2. Parametrizing elliptic curves	113
13.3. Some amazing identities	114
Chapter 14. Finding the lattice from the elliptic curve	115
14.1. The converse theorem	115
14.2. Why are they called “elliptic curves”	117
14.3. Transforming the j -function	117
14.4. What complex numbers map to $E(\mathbb{R})$?	117
14.5. The actual periods	118
14.6. Supersingular curves	119
Part 5. Torsion points	
Chapter 15. The subgroup of torsion points on an elliptic curve	125
15.1. The arithmetic of a torsion point	125
15.2. Torsion points in \mathbb{C} , and division polynomials	127
15.3. Other Λ -periodic functions	130

Chapter 16. Determining the torsion points on an elliptic curve	131
16.1. Embedding torsion in \mathbb{F}_p	131
16.2. The Tate module	133
16.3. Torsion points in \mathbb{F}_p	133
Part 6. Mordell's Theorem	
Chapter 17. Mordell's theorem for congruent number curves	137
17.1. Congruent numbers revisited	137
17.2. The converse Theorem for $E_A(\mathbb{Q})$	138
17.3. Mordell's Theorem: $E_A(\mathbb{Q})$ is finitely generated	139
Chapter 18. Mordell's theorem – $E(\mathbb{Q})$ is finitely generated	143
18.1. An explicit understanding of $E(\mathbb{Q})/2E(\mathbb{Q})$	143
18.2. The descent process; the proof of Mordell's Theorem	145
18.3. An upper bound on the rank	146
18.4. Remarks on large rank curves	146
Chapter 19. The Local-Global principle returns	147
19.1. Four squares in an arithmetic progression	147
19.2. The 2-Selmer group	148
19.3. A 3-descent?	149
19.4. A group action on curves	150
19.5. Selmer's curve	150
Chapter 20. Heights of rational points on elliptic curves	151
20.1. Bounds height when adding points	151
20.2. An inner product	152
20.3. The number of points in the Mordell-Weil lattice up to height x	153
Chapter 21. Applications of Mordell's theorem	155
21.1. Magic squares and elliptic curves	155
21.2. Problems involving powers and binomial coefficients	156
Part 7. Mordell's Theorem in general	
Chapter 22. Revision of basic tools of algebraic number theory	163
22.1. Solving the cubic. Pre-cursors	163
22.2. Fields	164
22.3. Integer solutions and quadratic fields	165
22.4. Galois theory	171
Chapter 23. Mordell's Theorem in number fields	175
23.1. Rational points in number fields	175

23.2. Torsion in number fields	177
Chapter 24. Fermat's Last Theorem	179
24.1. One way to prove Fermat's Last Theorem	179
24.2. Using congruences	181
24.3. A different descent	182
24.4. Second case of FLT	182
24.5. Criteria for FLT	183
Chapter 25. Singularities and bad reduction	185
25.1. Singular cubics over \mathbb{C}	185
25.2. Group laws	186
25.3. Reduction over different fields	186
Part 8. Applications and miscellaneous	
Chapter 26. Factoring and primality testing	191
26.1. Calculating $\#E(\mathbb{F}_p)$	191
26.2. Elliptic curves and factoring	192
26.3. Elliptic curves and primality testing	192
26.4. El Gamal, discrete logs, etc etc	193
Chapter 27. Combinatorics, partitions, and an example of modularity	195
27.1. Partitions	195
27.2. Generating functions for binary quadratic forms, and L -functions	195
27.3. Poisson's summation formula and Jacobi's theta function	196
27.4. Jacobi's powerful triple product identity	197
27.5. An example of modularity: $y^2 = x^3 - x$.	198
Part 9. Isogenies, endomorphisms and Galois representations	
Chapter 28. Isogenies over \mathbb{C}	203
28.1. Properties of isogenies	204
28.2. Dual isogenies	205
28.3. Explicit isogenies	206
Chapter 29. Isogenies over K	209
29.1. The shape of an isogeny	209
29.2. Separable isogenies over arbitrary fields	210
Chapter 30. Endomorphisms	213
30.1. Endomorphisms over \mathbb{C}	213
30.2. Degrees of endomorphisms	214
30.3. Algebra of endomorphisms	216

Nous espérons aller
jusqu'à le fin de partie
8 / We hope to get to
the end of part 8.

Chapter 31. Endomorphisms in $E(\overline{\mathbb{F}}_p)$	217
31.1. The Frobenius map	217
31.2. The number of points on $E(\mathbb{F}_p)$	218
31.3. The number of points on $E(\mathbb{F}_{p^k})$	219
31.4. Torsion points in \mathbb{F}_p	219
31.5. Isogenous curves	220
31.6. $\text{End}(E(\overline{\mathbb{F}}_p))$ when p is ordinary (that is, $t \neq 0$)	220
31.7. $\text{End}(E(\overline{\mathbb{F}}_p))$ when p is supersingular (that is, $t = 0$)	221
Chapter 32. The Hasse-Weil zeta function	223
32.1. A generating function for the number of points on $E(\mathbb{F}_{p^k})$	223
32.2. An alternative product for the local zeta function	224
32.3. Analytic properties of the Hasse-Weil L -function	224
Chapter 33. Representations	227
33.1. Endomorphisms acting on the Tate module	227
33.2. Galois representations	228
33.3. E with complex multiplication	229
Chapter 34. The field of rational functions of an elliptic curve	233
34.1. What functions are there on a curve?	233
34.2. The Weil pairing	234
34.3. Coincidence for different prime order torsion	235
Part 10. Lifting elliptic curves	
Chapter 35. Discussion of Deuring's Lifting lemma	239
35.1. The distribution of $\#E(\mathbb{F}_p)$ as we vary over elliptic curves E in \mathbb{F}_p	240
35.2. The distribution of $\#E(\mathbb{F}_p)$ as we vary over primes p , for a fixed elliptic curve E	240
35.3. Hecke's bound	240
35.4. Selberg's trace formula and Birch's formulae	240
35.5. Sato-Tate conjecture and Richard Taylor's Theorem	240
35.6. Lang-Trotter conjecture	240
Chapter 36. The infinitude of supersingular primes	241
36.1. Complex multiplication curves	241
Part 11. Modular Forms	
Chapter 37. Modular Forms	245
37.1. The magic of Eisenstein series	245
37.2. The Fourier expansion of an Eisenstein series	246

37.3. Modular forms	247
37.4. Determining spaces of modular forms	248
37.5. The j -function	250
37.6. The j -invariant and complex multiplication	251
37.7. Almost an Eisenstein series	252
37.8. Sublattice and subgroups	254
37.9. Hecke operators	255
37.10. The Mellin transform and the construction of L -functions	257
37.11. Congruence subgroups	259
Chapter 38. More easy modularity	261
Part 12. Singular Moduli	
Chapter 39. The Gross-Zagier formula	265
39.1. Special values of the j -function	265
39.2. Singular moduli and Gross-Zagier	265
Chapter 40. Ternary Quadratic Forms	267
40.1. Local-Global principle	267
40.2. Values taken and Iwaniec's theorem	267
Chapter 41. Equidistribution of Singular moduli	269
41.1. Duke's Theorem	269
Part 13. Heegner Points	
Chapter 42. Heegner points	273
42.1. Construction of Heegner points	273
42.2. Class number one via modular equations	273
Part 14. The Birch Swinnerton-Dyer conjecture	
Chapter 43. The Dirichlet class number formula	277
43.1. Dirichlet's class number formula	277
43.2. Quantitative local-global principle for integer solutions to Pell's equation	279
43.3. The size of a fundamental unit	279
43.4. The class number one problem in real quadratic fields	280
43.5. More L -functions: (Obtained from elsewhere)	280
43.6. to do	282
Chapter 44. The Birch Swinnerton-Dyer conjecture	283
44.1. Non-vanishing of central values	285

44.2.	Gross-Zagier fomula for $L'(E, 1)$ using Heegner point	285
44.3.	Towards a proof	286
Part 15. Further Diophantine problems		
Chapter 45.	Integral points on elliptic curves	289
45.1.	Taxicab numbers and other diagonal surfaces	289
45.2.	Sums of two cubes	290
45.3.	Thue's Theorem, etc. Baker's Theorem.	291
Chapter 46.	Higher degree equations	293
46.1.	The <i>abc</i> -conjecture	294
46.2.	Faltings' Theorem née Mordell's conjecture	295
46.3.	<i>abc</i> -conjecture	296
Chapter 47.	ArithmeticDynamics	297
47.1.	General discussion of unit groups	297
Chapter 48.	Distribution of ranks of elliptic curves	299
48.1.	The distribution of the rank(E_d) as we vary over non-zero E in \mathbb{F}_p	299
48.2.	Ranks and Galois theory	300
48.3.	Conjectural height bounds	301
48.4.	Conjectures by counting automorphisms	301
48.5.	Smith's "theorem"	301
Chapter 49.	The proof of Fermat's Last Theorem	303
49.1.	Eichler-Shimura and modularity	303
49.2.	Congruences for modular forms and FLT	303
49.3.	Selmer groups and Bhargava's program	303
Chapter 50.	Bibliography	305
Chapter 51.	Appendix – Belyi maps	307
51.1.	The non-existence of parametrized solutions, revisited	308
Chapter 52.	Appendix – Further failures of the local-global principle for cubics	311