

Cambridge University Press

978-0-521-64633-8 - The Algorithmic Resolution of Diophantine Equations

Nigel P. Smart

Table of Contents

[More information](#)

Contents

| | |
|---|-----------|
| Preface | xi |
| Outline | xii |
| Computer packages | xv |
| Notation | xv |
| Thanks | xvi |
| Chapter I. Introduction | 1 |
| I.1. A brief history | 2 |
| I.2. Algorithms | 7 |
| I.3. What is a diophantine equation? | 9 |
| I.4. An elliptic curve | 10 |
| Part 1. Basic solution techniques | 15 |
| Chapter II. Local methods | 17 |
| II.1. p -adic numbers | 17 |
| II.2. p -adic numerical analysis | 23 |
| II.3. Exercises | 32 |
| Chapter III. Applications of local methods to diophantine equations | 33 |
| III.1. Applications of Strassmann's theorem | 33 |
| III.2. Skolem's method | 36 |
| III.3. The Hasse principle | 39 |
| III.4. Finding small solutions | 40 |
| III.5. Exercises | 43 |
| Chapter IV. Ternary quadratic forms | 45 |
| IV.1. A normal form | 45 |
| IV.2. Local solubility | 46 |
| IV.3. Global solubility | 49 |
| IV.4. New solutions for old | 53 |
| IV.5. Exercises | 56 |
| Chapter V. Computational diophantine approximation | 59 |
| V.1. Continued fractions | 59 |
| V.2. Approximation lattices | 64 |
| V.3. Lattices | 65 |
| V.4. The LLL-algorithm | 71 |

Cambridge University Press

978-0-521-64633-8 - The Algorithmic Resolution of Diophantine Equations

Nigel P. Smart

Table of Contents

[More information](#)

| | | |
|----------------|--|-----------|
| viii | CONTENTS | |
| V.5. | Exercises | 75 |
| Chapter VI. | Applications of the LLL–algorithm | 77 |
| VI.1. | A ‘fun’ application | 77 |
| VI.2. | Knapsack problems | 79 |
| VI.3. | Approximating linear forms | 82 |
| VI.4. | p -adic analogues | 87 |
| VI.5. | Exercises | 93 |
| Part 2. | Methods using linear forms in logarithms | 95 |
| Chapter VII. | Thue equations | 97 |
| VII.1. | Thue equations | 97 |
| VII.2. | $X^4 - 2Y^4 = \pm 1$ | 105 |
| VII.3. | The method of Bilu and Hanrot | 108 |
| VII.4. | Integral points on elliptic curves (I) | 111 |
| VII.5. | $Y^2 = X^3 - 6X - 14$ | 113 |
| VII.6. | Exercises | 116 |
| Chapter VIII. | Thue–Mahler equations | 117 |
| VIII.1. | Thue–Mahler equations | 117 |
| VIII.2. | The prime ideal removing lemma | 118 |
| VIII.3. | The method | 119 |
| VIII.4. | $X^3 - X^2Y + XY^2 + Y^3 = \pm 11^s$ | 124 |
| VIII.5. | Exercises | 132 |
| Chapter IX. | S -unit equations | 133 |
| IX.1. | S -unit equations | 133 |
| IX.2. | Sieving | 141 |
| IX.3. | An S -unit equation in a cyclic quintic field | 146 |
| IX.4. | Integral points on elliptic curves (II) | 150 |
| IX.5. | Other applications | 151 |
| IX.6. | Exercise | 152 |
| Chapter X. | Triangularly connected decomposable form equations | 153 |
| X.1. | Triangularly connected linear forms | 153 |
| X.2. | TCDF equations | 155 |
| X.3. | Solving TCDF equations | 156 |
| X.4. | Exercises | 163 |
| Chapter XI. | Discriminant form equations | 165 |
| XI.1. | Discriminant and index forms | 165 |
| XI.2. | The general case: discriminant forms as TCDFs | 167 |
| XI.3. | A discriminant form equation in a cyclic quintic field | 169 |
| XI.4. | Special cases | 170 |
| XI.5. | Exercises | 174 |

Cambridge University Press

978-0-521-64633-8 - The Algorithmic Resolution of Diophantine Equations

Nigel P. Smart

Table of Contents

[More information](#)

| CONTENTS | ix |
|--|-----|
| Part 3. Integral and rational points on curves | 175 |
| Chapter XII. Rational points on elliptic curves | 177 |
| XII.1. Basics on elliptic curves | 177 |
| XII.2. The weak Mordell–Weil theorem | 182 |
| XII.3. The Mordell–Weil theorem | 190 |
| XII.4. A conditional algorithm | 192 |
| XII.5. Exercises | 194 |
| Chapter XIII. Integral points on elliptic curves | 197 |
| XIII.1. Elliptic logarithms | 197 |
| XIII.2. Elliptic integrals and the <i>AGM</i> | 198 |
| XIII.3. Integral points | 202 |
| XIII.4. Integral points on the curve $Y^2 = X^3 - 2$ | 206 |
| XIII.5. <i>S</i> -integral points | 207 |
| XIII.6. Other methods and problems | 210 |
| XIII.7. Exercises | 211 |
| Chapter XIV. Curves of genus greater than one | 213 |
| XIV.1. Curves and their Jacobians | 213 |
| XIV.2. Hyperelliptic curves and their Jacobians | 215 |
| XIV.3. Rational points on curves of genus greater than one | 217 |
| XIV.4. Integral points on hyperelliptic and superelliptic curves | 219 |
| XIV.5. Fermat curves | 221 |
| XIV.6. Catalan’s equation | 222 |
| XIV.7. Exercises | 224 |
| Appendix A. Linear forms in logarithms | 225 |
| A.1. Linear forms in complex logarithms | 225 |
| A.2. Linear forms in <i>p</i> -adic logarithms | 225 |
| A.3. Linear forms in elliptic logarithms | 226 |
| Appendix B. Two useful lemmata | 229 |
| References | 231 |
| Index | 241 |