

# Contents

|   |     |
|---|-----|
| <i>Acknowledgements</i>   | vii |
| <i>Introduction</i>   | 1   |
| 1. Historical overview  | 5   |
| 1.1 18 <sup>th</sup> Century — a prologue . . . . .                           | 5   |
| 1.2 19 <sup>th</sup> century — the classical period . . . . .                 | 6   |
| 1.3 Early 20 <sup>th</sup> century — arithmetic applications . . . . .        | 7   |
| 1.4 Later 20 <sup>th</sup> century — the link to elliptic curves . . . . .    | 8   |
| 1.5 The 21 <sup>st</sup> century — the Langlands Program . . . . .            | 9   |
| 2. Introduction to modular forms  | 11  |
| 2.1 Modular forms for $SL_2(\mathbf{Z})$ . . . . .                            | 11  |
| 2.2 Eisenstein series for the full modular group . . . . .                    | 15  |
| 2.3 Computing Fourier expansions of Eisenstein series . . . . .               | 17  |
| 2.4 Congruence subgroups . . . . .  | 21  |
| 2.5 Fundamental domains . . . . .   | 25  |
| 2.6 Modular forms for congruence subgroups . . . . .                          | 28  |
| 2.7 Eisenstein series for congruence subgroups . . . . .                      | 32  |
| 2.8 Derivatives of modular forms . . . . .                                    | 35  |
| 2.8.1 Quasi-modular forms . . . . .   | 37  |
| 2.9 Exercises . . . . .   | 38  |
| 3. Results on finite-dimensionality   | 41  |
| 3.1 Spaces of modular forms are finite-dimensional . . . . .                  | 41  |
| 3.2 Explicit formulae for the dimensions of spaces of modular forms . . . . . | 46  |

|       |   |     |
|-------|---|-----|
| 3.2.1 | Formulae for the full modular group . . . . .   | 46  |
| 3.2.2 | Formulae for congruence subgroups . . . . .   | 49  |
| 3.3   | The Sturm bound . . . . .   | 52  |
| 3.4   | Exercises . . . . .   | 55  |
| 4.    | The arithmetic of modular forms . . . . .   | 57  |
| 4.1   | Hecke operators . . . . .   | 58  |
| 4.1.1 | Motivation for the Hecke operators . . . . .  | 58  |
| 4.1.2 | Hecke operators for $M_k(\mathrm{SL}_2(\mathbf{Z}))$ . . . . .                                | 59  |
| 4.1.3 | Hecke operators for congruence subgroups . . . . .  | 63  |
| 4.2   | Bases of eigenforms . . . . .   | 69  |
| 4.2.1 | The Petersson scalar product . . . . .  | 69  |
| 4.2.2 | The Hecke operators are Hermitian . . . . .   | 75  |
| 4.2.3 | Integral bases . . . . .  | 79  |
| 4.3   | Oldforms and newforms . . . . .   | 80  |
| 4.3.1 | Multiplicity one for newforms . . . . .   | 85  |
| 4.4   | Exercises . . . . .   | 88  |
| 5.    | Applications of modular forms . . . . .   | 93  |
| 5.1   | Modular functions . . . . .   | 94  |
| 5.2   | $\eta$ -products and $\eta$ -quotients . . . . .  | 98  |
| 5.3   | The arithmetic of the $j$ -invariant . . . . .  | 103 |
| 5.3.1 | The $j$ -invariant and the Monster group . . . . .  | 106 |
| 5.3.2 | “Ramanujan’s Constant” . . . . .  | 107 |
| 5.4   | Applications of the modular function $\lambda(z)$ . . . . .                                   | 108 |
| 5.4.1 | Computing digits of $\pi$ using $\lambda(z)$ . . . . .  | 109 |
| 5.4.2 | Proving Picard’s Theorem . . . . .  | 111 |
| 5.5   | Identities of series and products . . . . .   | 112 |
| 5.6   | The Ramanujan-Petersson Conjecture . . . . .  | 113 |
| 5.7   | Elliptic curves and modular forms . . . . .   | 116 |
| 5.7.1 | Fermat’s Last Theorem . . . . .   | 119 |
| 5.8   | Theta functions and their applications . . . . .  | 120 |
| 5.8.1 | Representations of $n$ by a quadratic form in an<br><i>even</i> number of variables . . . . . | 121 |
| 5.8.2 | Representations of $n$ by a quadratic form in an <i>odd</i><br>number of variables . . . . .  | 128 |
| 5.8.3 | The Shimura correspondence . . . . .  | 131 |
| 5.9   | CM modular forms . . . . .  | 133 |

|       |  |     |
|-------|--|-----|
| 5.10  | Lacunary modular forms . . . . .   | 135 |
| 5.11  | Exercises . . . . .  | 138 |
| 6.    | Modular forms in characteristic $p$  | 143 |
| 6.1   | Classical treatment . . . . .  | 143 |
| 6.1.1 | The structure of the ring of mod $p$ forms . . . . .                         | 144 |
| 6.1.2 | The $\theta$ operator on mod $p$ modular forms . . . . .                     | 150 |
| 6.1.3 | Hecke operators and Hecke eigenforms . . . . .                               | 151 |
| 6.2   | Galois representations attached to mod $p$ modular forms .                   | 152 |
| 6.3   | Katz modular forms . . . . .   | 156 |
| 6.4   | The Sturm bound in characteristic $p$ . . . . .                              | 158 |
| 6.5   | Computations with mod $p$ modular forms . . . . .                            | 159 |
| 6.6   | Exercises . . . . .  | 161 |
| 7.    | Computing with modular forms   | 163 |
| 7.1   | Historical introduction to computations in number theory                     | 163 |
| 7.2   | MAGMA . . . . .  | 167 |
| 7.2.1 | MAGMA philosophy . . . . .   | 170 |
| 7.2.2 | MAGMA programming . . . . .  | 171 |
| 7.3   | SAGE . . . . .   | 173 |
| 7.3.1 | SAGE philosophy . . . . .  | 175 |
| 7.3.2 | SAGE programming . . . . .   | 175 |
| 7.3.3 | The SAGE interface . . . . .   | 176 |
| 7.3.4 | SAGE graphics . . . . .  | 177 |
| 7.4   | PARI and other systems . . . . .   | 177 |
| 7.4.1 | PARI . . . . .   | 177 |
| 7.4.2 | Other systems and solutions . . . . .  | 179 |
| 7.5   | Discussion of computation . . . . .  | 180 |
| 7.5.1 | Computation today . . . . .  | 180 |
| 7.5.2 | Expected running times . . . . .   | 182 |
| 7.5.3 | Using computation effectively . . . . .                                      | 183 |
| 7.5.4 | The limits of computation . . . . .  | 184 |
| 7.5.5 | Guy's law of small numbers . . . . .   | 187 |
| 7.5.6 | How hard is it to calculate Fourier coefficients of modular forms? . . . . . | 189 |
| 7.6   | Exercises . . . . .  | 189 |
| 7.6.1 | MAGMA . . . . .  | 190 |
| 7.6.2 | SAGE . . . . .   | 191 |

|            |   |     |
|------------|---|-----|
| 7.6.3      | PARI . . . . .                          | 193 |
| 7.6.4      | MAPLE . . . . .                         | 193 |
| Appendix A | MAGMA code for classical modular forms  | 195 |
| Appendix B | SAGE code for classical modular forms   | 197 |
| Appendix C | Hints and answers to selected exercises | 199 |
|            | <i>Bibliography</i>                     | 205 |
|            | <i>List of Symbols</i>                  | 217 |
|            | <i>Index</i>                            | 221 |