

Introduction

This book is based on notes for lectures given at the Mathematical Institute at the University of Oxford over the three years 2004—2007; as a graduate course both in 2004—2005 and in 2006—2007, and as the undergraduate course *Introduction to Modular Forms* in 2005—2006.

This book

This book focuses on the computational aspects of the theory of modular forms much more than most other books do. It is designed to be an introduction to these computational aspects of the theory. Computational algebra packages like MAGMA and SAGE can (for instance) compute Fourier expansions of modular forms and modular functions to an extremely high precision; this book will hopefully help the student to use computers to deepen their understanding of modular forms and number theory.

It also gives a grounding in the theory of classical modular forms, starting with modular forms for $SL_2(\mathbf{Z})$, and progressing to modular forms of higher level, modular functions, half-integral weight modular forms and mod p modular forms. The two aspects are intended to complement each other, each helping to motivate and inspire the other.

Possible courses

The courses that this book is based upon were all 16-lecture courses, given over one Oxford term. The undergraduate course was given to final-year undergraduate students and to students taking a one-year taught Master's course.

This book concentrates on the computational aspects of the theory of modular forms, but at the same time also gives a grounding in the classical and theoretical aspects of modular forms. We now list some possible courses which could be given based upon this book.

One possible way to give a course using this book would involve teaching students essentially only about modular forms for the full modular group, as [Serre (1973a)] does, in a broadly “traditional” way. This could still include interesting arithmetic, such as a study of the Ramanujan τ function and the j -invariant, but avoids the complication of higher levels. There are some projects in the computational chapter which could be used to stretch the more able students and also serve as inspiration for end-of-course projects, especially for beginning graduate students.

If the instructor has more time, then the theory of modular forms for congruence subgroups of $SL_2(\mathbf{Z})$ could also be introduced. This would allow the introduction of many well-known modular forms, such as those associated to elliptic curves, many η -products, and theta functions. The work of Wiles and Taylor in proving the modularity conjecture, and hence Fermat’s Last Theorem, is of great public interest, and the general concepts of the proof can be presented.

Another possible course would be one focused on introducing students to computational number theory, using modular forms as motivational examples. This might include teaching students about MAGMA, PARI and SAGE, as well as giving them an overview of the history of computation. End-of-course projects for this course could include more or less programming to suit the instructor and the level of the students. The graphically inclined could write programs similar to those of Verrill [Verrill (2001)] to create pictures of fundamental domains, or use the graphics creation facilities of PARI and SAGE to create other graphics.

A third possibility would be to teach a course dealing with theta functions, starting with their history (see, for example, [Glaisher (1907a,b,c)], for early computational results) and continuing to modern-day work. This course could balance theoretical work showing that theta functions really are modular forms with computations of explicit theta functions, and more advanced students could read books like [Miyake (2006)] which give more details on this subject.

The instructor could also teach a course emphasizing the applications of modular forms in number theory and elsewhere. It is important to realize that, despite their definition as holomorphic functions from \mathcal{H} to \mathbf{C} , modular forms have a rich number-theoretic theory, and Chapter 5 gives a

sample of some of the many and varied results that rely on the theory of modular forms.

An overview of this book¹

We encourage the reader of this book to use their favourite computer algebra package (such as MAGMA or SAGE) to compute examples as they read, to help them develop their intuition. The best way to learn how to use such a package is to experiment with it to find out how it works; Chapter 7 gives an introduction and brief overview, but there is no substitute for hands-on experience.

The chapters cover the theory in the following way; Chapter 2 gives the definition of a modular form for $SL_2(\mathbf{Z})$, and prove that modular forms exist (which is not obvious to the newcomer to the subject). We also define fundamental domains and modular forms for congruence subgroups.

In Chapter 3, we consider modular forms as complex-analytic objects, and use this aspect of their character to prove that spaces of modular forms of a given weight for a given congruence subgroup are finite-dimensional. Following on from this, in Chapter 4 we introduce the Hecke operators, which are linear operators acting on spaces of modular forms, and prove results about them. We note that these operators explain the recurrence relations that the coefficients of $\Delta(q)$ satisfy, for instance.

We then apply the results derived in these chapters in Chapter 5 to a variety of applications, such as Fermat's Last Theorem, computing digits of π , and computing the number of representations of integers by quadratic forms. We also introduce the concept of mod p modular forms in Chapter 6, give structure theorems for mod p modular forms, and talk about Serre's Conjecture, which has been proved very recently.

Finally, we consider the practical side of computation in Chapter 7; after giving a brief introduction to the history of computations in the world of number theory, which includes such highlights as the Lehmer bicycle-chain sieve, we introduce the computer algebra packages MAGMA, SAGE and PARI, and briefly touch on the theoretical side of computing in mathematics. The book ends with appendices containing examples of code for the algebra packages discussed in the text.

¹Many books have a section of this nature. We note that [Lamport (1994)] is one of the very few that has a section called "How to Avoid Reading This Book".