Preface

This book was developed from the notes for a one semester introductory course on elliptic curves. The theory of elliptic curves has a long history (even the name "elliptic curves" was chosen for historical reasons, the actual relation with ellipses is tenuous at best). Today it appears in many different contexts, some of which are far removed from the origins of the subject. Its long history, as well as the current interest in elliptic curves, makes it very difficult to find material to present in an introduction that has not already been covered in other sources. These notes make no pretension of doing that. For a one semester course one must however make a careful and limited choice. The choice made for this course was dictated to a large extent by the heterogeneous nature of the audience. This audience consisted on the one hand of mathematics students, at various stages of their education, but generally with a number theoretic interest, and on the other hand of computer science students interested in the cryptographic aspects of elliptic curves. This led me from the beginning to assume as little background knowledge as possible while at the same time limiting the background material given in the course. For instance, I define the notion of analytic and meromorphic functions and prove the maximal principle, but I only mention without proof some basic results on uniform convergence of holomorphic functions. The basic idea was to give the audience an appreciation of how difficult the applicable results are, while not necessarily proving all of them. Similarly, no knowledge of algebraic geometry was assumed.

No matter the reason for being interested in elliptic curves, knowledge of basic analytic methods is indispensable. Consequently we start by discussing some of the analytic aspects of elliptic curves. We roughly follow the historical development, starting with elliptic integrals and Euler's addition theorem, then turning to elliptic functions where the power of the analytic methods is demonstrated when we prove the fundamental formulas for the Weierstrass $\wp$-function. Preparing for a more algebraic approach we give a short introduction to the projective plane. Then we discuss equivalences between elliptic curves and lattices, leading up to the j-function and its incarnation as both a rational expression in the coefficients of the equation defining the elliptic curve and as an analytic function in the lattice (also defining the elliptic curve).

We then turn to some more specialised subjects reflecting the interests of the audience described above. To prepare for a student presentation of Schoof's algorithm for counting the number of points on an elliptic curve, we went through the basic properties of the division polynomials. We then finished with some additional number theoretical aspects; curves with complex multiplication and the use of modular forms for proving Jacobi's formula for the number of representations of a positive integer as a sum of four squares.

At several points we need to do some reasonably complicated numerical or algebraic calculations. It can be argued that one should avoid such a situation as it obscures

what is going on. In most cases these situations are indeed avoidable but at the cost of having to develop more theory. (Note however that in a few cases the calculations seem unavoidable, even using more high powered machinery. The calculations of Subsection 11.1.1 is one such example.) Within the confines of a one semester course this is not however possible. I have chosen the middle road of leaving the heavy calculations to the Mathematica computer algebra system. A Mathematica notebook containing these calculations is available http://www.math.su.se/~teke/undervisning/Elliptisk.nb and the computations can be performed by the reader using Mathematica, but the notebook can also be viewed using the freely available MathReader program (which can be downloaded from http://www.wolfram.com).