PREFACE

Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.

Paul Erdős

Geometry and the theory of numbers are as old as some of the oldest historical records of humanity. Since Euclid's *Elements* and Diophantus's *Arithmetica*, many excellent geometry and number theory texts have been written, including timeless classics such as [**HW38**]. As we shall lay out in more detail in Chapter 1, the approach of this book is slightly different from more traditional sources, in that the emphasis is in the interactions of number theory with geometry. The field of *arithmetic geometry*, which appears in the subtitle of this book, is indeed the study of the intersection of number theory (arithmetic) and algebraic geometry. The author's reason for this more geometric point of view is the following. Some of the traditional number theory textbooks may seem (to the student) a list of topics, each of which may be of important historical value but that do not readily appear to form a coherent set of topics, well integrated with each other (e.g., prime numbers, congruences, perfect numbers, quadratic reciprocity, and continued fractions). Of course, number theorists understand that these topics are deeply interconnected, and one way to highlight the interwoven nature of number theory is through geometry. In this text, the goal is to use geometry as the motivation to prove the main theorems in the book. For example, the fundamental theorem of arithmetic (the fact that every integer $n \geq 2$ has a unique factorization as a product of prime numbers) is a consequence of the tools we develop in order to find all the integral points on a line in the plane (i.e., the points (x_0, y_0) on a line $L : ax + by = c$ with integer coordinates x_0 and y_0). Similarly, Gauss's law of quadratic reciprocity and the theory of continued fractions naturally arise when we attempt to determine the integral points on a curve in the plane given by a quadratic polynomial equation.

In Chapter 1 we give a brief overview of the types of diophantine equations (i.e., systems of equations given by polynomials) that are the objects of study. The rest of the book is structured in three acts that correspond to linear, quadratic, and cubic curves, respectively.

(I) In Part 1 we introduce the basic tools of number theory. In particular, we discuss the integers and prime numbers and develop the theory of (linear) congruences. We also introduce some basic concepts of abstract algebra (groups, rings, fields) using congruence classes as a motivating example. These tools are applied to determine rational solutions of polynomials in one variable and the integral and rational points on lines in the plane.

(II) In Part 2 we study quadratic equations in one and two variables. We develop the theory of quadratic congruences, we describe the theorem of Hasse and Minkoswki (without a proof), and we also introduce continued fractions. The material is then used to find the integral and rational points on conics: parabolas, ellipses, and hyperbolas.

(III) Part 3 is a brief introduction to the theory of cubic curves. After discussing the projective line and projective space and learning how to work with singular cubic curves, we concentrate on non-singular cubics, and we give a summary of the theory of elliptic curves (projective non-singular cubic curves with at least one rational point).

A number of chapters end with applications of the theory to other topics and, in particular, we highlight the cryptographic applications in Sections 4.6.4, 7.5.3, 8.9.1, 10.7.2, and 16.9.

The book contains much more material than can be covered in a one-semester undergraduate course. For a first course in number theory or arithmetic geometry, we recommend covering Chapters 1 through 10 (Chapter 6 on finite fields is optional). For a second course in arithmetic (or diophantine) geometry, the instructor can cover Chapters 9 through 16 (Chapter 11 on the Hasse–Minkowski theorem is optional). The text assumes that the student has had a sequence of courses in calculus, up to multivariable calculus (a familiarity with matrices is assumed in some exercises). It is recommended that the student has seen an introduction to proofs before reading this book. However, the first few chapters have the secondary goal of providing practice in proof-writing, and they include a review of proofs by induction, in particular.

The material in this text ends where [**Loz11**] begins. There are, of course, many other undergraduate sources on number theory that are highly recommended: [**AC95**], [**Bur10**], [**Chi95**], [**Con1**], [**Gou97**], [**HW38**], [**HPS14**], [**Ros10**], [**ST92**], [**Sil12**], [**Ste08**], [**Was08**], and [**Wei17**], among many others. At the graduate level, the volumes [**DF03**], [**IR98**], [**Lor96**], [**Mil06**], [**Ser73**], and [**Sil86**] are excellent introductions to various aspects of algebra, number theory, and arithmetic geometry.

I started writing my own notes when I taught elementary number theory courses at Cornell University (in the fall of 2006 and 2007) and at the University of Connecticut (in the fall of 2008 and 2011 and the spring of 2014). This book grew out

of these notes and the lectures of a special topics course (on diophantine geometry) that I taught at UConn in the fall of 2012. I would like to thank Keith Conrad for many suggestions and corrections. Also, I would like to thank the UConn undergraduate students in my class "MATH 3240Q: Introduction to Number Theory" for carefully reading my notes and providing useful feedback and criticism. In particular, I would like to thank Lia Bonacci, Heather Clinton, Jeremy Driscoll, Randolph Forsyth, Carly Gaccione, Taylor Garboski, Tom Jones, Gregory Knight, David Khondkaryan, Pravesh Mallik, Nicole Raymond, Heather Risley, Antonio Rossini, and Rachel Tangard for their comments, and special thanks go to Michael Lau and Byron Sitaras for their many and very detailed comments. Finally, I would like to thank Jason Dorfman (CSAIL/MIT), the Wikimedia Commons, and the Archives of the Mathematisches Forschungsinstitut Oberwolfach for their permission to use the images from their collections that appear in this book.