Preface

A question implicit in many conversations with undergraduates at first-year orientation is, “If I were to take only one mathematics class, what should it be?” Of course, there is no one correct answer. A more interesting question (not that it gets asked) might be, “Is there a class which introduces me to the subject of mathematics?” In answer, some might proffer various discrete/finite math/introduction to proof courses, but I think these are not really an answer to that question. A number of years ago, our department was interested in providing a wide variety of courses which attempted to answer that question, and this book details one such offering.

Therefore, one goal of this book is to present some of the vista of modern mathematics to undergraduates who have just started their mathematical careers, with the intent of enticing (and guiding) them into taking mathematics courses beyond the typical calculus regime. As mathematicians, we have acquired the perspective that mathematics represents not only a broad collection of tools which can be brought to bear to solve a myriad of problems, but more interestingly, that the various subdisciplines in mathematics are interconnected often in surprising ways, adding immensely to the richness and allure of the discipline itself. Undergraduates beginning their careers certainly do not have that perspective, and if they are lucky, they begin to acquire it only near the end of their undergraduate majors. The hope in writing this book is to provide some of that perspective to students at an early stage in their careers so as both to (re)excite them about mathematical exploration, and to help inform their choices as they go forward in their undergraduate experience.

The focal point for this text is to lead students to understand the arithmetic of elliptic curves over a finite field and some applications of elliptic curves to modern cryptography. Assuming only calculus as prerequisite, there is a great deal of ground to cover, but a wonderful opportunity to demonstrate how many areas of mathematics are intertwined.

That said, this book is not (nor is it intended to be) a typical textbook in many respects. While the topics introduced include material on elementary number theory, abstract algebra, cryptography, affine and projective geometry, the intent is not to present a thorough introduction to any of those subjects; it is meant to generate interest in exploring those subjects in more detail. Excellent books devoted individually to those topics are plentiful, but typically they are aimed at a more mathematically sophisticated audience.

This book aims at a mathematically young audience, one that more likely than not has never seen a substantive mathematical proof. Indeed, the only real prerequisite for this book is some one-variable calculus; the rest of the mathematical topics are introduced on-the-fly. This is also not a standard textbook in another important sense. Instead of presenting succinct proofs of results (as is done in a typical textbook), many proofs are presented more as explorations, including (on occasion) some intentional peeks down blind alleys. That is to say, this book makes a significant effort to teach students about how to produce or discover a proof, by presenting mathematics as an exploration. Indeed, while somewhat of a cliché, the book is a great deal more about the journey than the destination, and it is intended to point to the many branches off the main path to be explored in the future.

In the end, the book seems to serve several purposes. It serves, as initially conceived, as a means of introducing many topics in modern mathematics with interconnections among them to motivate students to take more mathematics. It also seems well suited to serve as an alternate course introducing proofs and abstract mathematics, which occupies a prominent place in many mathematics programs. And finally, given that one cannot really understand modern cryptography without some of its mathematical underpinnings, this book is well suited to computer science programs which desire to offer a course investigating the practical and implementation sides of cryptography, but which need their students to have some semblance of its necessary mathematical background.

Introduction

This book is written to introduce a student with only single-variable calculus as background to enough mathematics to understand the basics of elliptic curves over finite fields and their applications to modern cryptography. Topics include basic notions in elementary number theory and abstract algebra, aspects of affine and projective geometry, as well cryptography and cryptanalysis. The goal of this book is not so much to provide complete answers to the questions we raise as it is to show the many connections between those questions and areas of mathematics whose further study will provide deeper answers.

In Chapter 1 we give a cursory exposition of three problems in number theory which are connected to elliptic curves: Fermat's Last Theorem, the congruent number problem, and applications of number theory to cryptography.

Chapter 2 is quite broad, recasting problems in number theory as problems amenable to geometric or algebraic interpretation. We look at connections of congruent numbers to Pythagorean triples, and at connections between Pythagorean triples and rational points on the unit circle. We explore in detail how to parametrize the rational points on the unit circle and use the parametrization to produce a simple algorithm to enumerate square-free congruent numbers. Then we begin to look for structure inherent in certain sets. For example, we know the set of points in $\mathbb{R}^3$ that satisfy $x + y + z = 0$ has the geometric structure of a plane through the origin. The set of rational points that satisfy the same equation does not seem to have geometric structure, but it does still have algebraic structure once we define the notion of vector space. We give a few examples that characterize the notion of dimension of a space along with the notion of basis, which, while clearly important in their own right, also foreshadow the rank of a finitely generated abelian group, the group of rational points on an elliptic curve.

We talk about rational points on more general curves and give Bachet's duplication formula for the elliptic curves $y^2 = x^3+k$, $k \neq 0$; this is one of the few places we use some calculus. Beyond that, we work to gain insight into Bézout's theorem concerning the number of points of intersection of two plane curves. We see how the issues of the field of definition and multiplicity affect the answer and hint that this is still not enough to give a complete answer, suggesting a future need to expand our view from affine to projective space.

Chapter 3 is rather traditional, introducing basic concepts in elementary number theory including divisibility, gcd, and division and Euclidean algorithms. We take a first pass at modular arithmetic, noting that congruence is an equivalence relation. We give some simple applications of modular arithmetic, and we use the Caesar cipher both as another application and as a vehicle to introduce some standard terminology in cryptography. We extend Caesar ciphers to affine ones and explore conditions under which affine transformations can function as encryption algorithms. This leads to determining the conditions under which linear congruences can be solved and to determining the number of incongruent solutions. All this is preparatory to the next chapter where we talk about the set of residues modulo n having an algebraic structure.

Chapter 4 is another in which we slowly unravel many important ideas that lead to the characterization of $\mathbb{Z}_n$ (the set of residues modulo n) as a ring and U_n (the set of reduced residues modulo n) as its unit group. We begin by understanding the standard arithmetic operations on the integers as binary operations on the set $\mathbb{Z}$ and how their properties endow $\mathbb{Z}$ with the structure of a commutative ring, passing through the notion of a group on the way. Then we use arithmetic with fractions ($\mathbb{Q}$) to motivate binary operations on a set of equivalence classes. Armed with that intuition, we define congruence classes modulo n, and show that there are well-defined binary operations which can be defined on them which make the set of residues $\mathbb{Z}_n$ into a commutative ring with identity. We then show that we can make the set of reduced residues (the units of $\mathbb{Z}_n$) into an abelian group. We define the Euler totient function ϕ and prove Euler's theorem and Fermat's little theorem, which we will need to justify that RSA (the Rivest–Shamir–Adelman algorithm) functions as intended. We discuss modular exponentiation, and end with an application to factoring, Pollard's $p - 1$ method which serves as the model against which we compare Lenstra's elliptic curve method of factorization.

Chapter 5 begins with a simple description of how public-key cryptography facilitates the creation of a secure connection when making an online purchase. Then we discuss more of the fundamentals of a public-key cryptosystem, followed by a discussion of signatures and authentication. We then begin to make things somewhat more realistic by talking about hash functions and signatures applied to a hash. We discuss the use of hash functions in daily use and specific requirements for hash functions in current use. We discuss preimage resistance problems in relation to the Birthday paradox in probability. The chapter ends with some security considerations for RSA.

Chapter 6 introduces a bit more algebra, including the notion of a cyclic group and the fundamental theorem of finite abelian groups. We use the fundamental theorem to give a proof that for p a prime, the set of reduced residues U_p is cyclic, leading to a discussion of primitive roots. This in turn leads to the notion of discrete logarithms, the Diffie–Hellman key exchange, and ElGamal encryption.

Chapter 7 covers a great deal of ground beginning with a gradual introduction to projective space. We discuss how and why to homogenize a polynomial defining an affine plane curve so as to reveal extra points on the corresponding projective curve. Then we take a significant amount of time to define the group law for the set of points on an elliptic curve, and we abstract from it the algebraic formulas that define the addition law in projective space. We give several examples where we determine the isomorphism class of the abelian group of points of an elliptic curve over a finite field, and we end with Hasse's theorem bounding the number of points on an elliptic curve over the finite field $\mathbb{F}_p$. As an application, we show that the probability that a randomly chosen $x \in \mathbb{F}_p$ is the x-coordinate of a point on the elliptic curve is approximately one-half, which we use in the last chapter in discussing an elliptic curve version of Diffie–Hellman and the ElGamal cryptosystem.

In the final chapter we look at applications of all our work thus far. We introduce Lenstra's elliptic curve method (ECM) of factorization and discuss its analogy with Pollard's $p - 1$ method. We then talk about how to embed a plaintext message as a point on an elliptic curve and, given that embedding, what would be the appropriate analogs of Diffie–Hellman and ElGamal. We end with some interesting remarks about the NSA's vision and recommendations regarding cryptography in a post-quantum computer world.

Appendix A completes the discussion of some themes that motivated much of the exposition, but the level of exposition is now far above where it has been in the body of the text. Giving closure to the topic of congruent numbers is Tunnell's theorem whose solution involves a discussion of Mordell's theorem on the structure of $E(\mathbb{Q})$, the set of rational points on an elliptic curve, as well as the Birch and Swinnerton-Dyer conjecture. The appendix ends with a brief discussion of elliptic curves over $\mathbb{C}$, elliptic functions, and the characterization of $E(\mathbb{C})$ as a complex torus.

Appendix B has solutions to the majority of exercises posed in the text.

All code and figures in the text were produced with Sage [**S$^+$15**].