Preface

Imagine that you could go back in time, say 65 million years, and there you are, standing on top of a mountain overseeing a large pond around which there are 13 dinosaurs drinking from the pond. Yes, 13, a prime number. But wait a minute, prime numbers have not been invented yet, right ? Nevertheless, there are 13 dinosaurs right there in front of you ! The reason is that prime numbers have always existed: they are not an invention of mankind. In fact, if there is some other civilization out there in the Universe, perhaps the prime number theorem – which says that the number of primes up to x is roughly $x/\log x$ – is known to its inhabitants. Well, Hollywood certainly thinks so: recall the movie *Contact* featuring an astrophysicist played by Jodie Foster and based on a famous novel by Carl Sagan. In that movie, humans receive a message from outer space which starts by listing the prime numbers 2, 3, 5, 7, up to 101. Yes, mathematics is a universal language, and prime numbers are a good demonstration of this. Moreover, their study is vast, boundless and fascinating.

So, this book is about the life of primes. Indeed, once they are defined, primes begin a life on their own: a prime is an integer larger than 1 whose only divisors are 1 and itself. Given this definition, primes start living. The mysteries surrounding primes begin multiplying just like living cells reproduce themselves, and there seems to be no end to it.

Why the fascination for prime numbers? One of the reasons that people are attracted to the study of prime numbers is that although most problems regarding primes can be stated in simple terms – just think of the twin prime conjecture which states that there are infinitely many primes p such that $p+2$ is also a prime and which has challenged professional and amateur mathematicians for centuries – their analysis and solutions often require much thinking and great ingenuity.

A journey through time

Many number theory books include the study of prime numbers. Most of them were written for teaching purposes, and others for the pleasure of the general public. These should make everyone happy, right? So why another book on primes? Our monograph offers a somewhat different perspective. Besides covering some of the most important results regarding prime numbers, we present a range of problems number theorists are currently working on and the references that will allow the curious reader to further investigate some of these problems. Moreover, we selected topics related to primes that will appeal to those mathematicians who wish to enrich their general mathematical culture. We have also chosen to present the topics in chronological order, as they have emerged throughout history. Although we do not claim to provide a thorough history of number theory, we do shed light on the humans who contributed to the life of primes. Indeed, history does help understand how mathematical results evolved over time. Recall the 1675 statement attributed to Isaac Newton: "If I have seen further, it is by standing on the shoulders of Giants". Indeed, theorems do not simply pop up suddenly. They are for the most part the final outcome of many attempts by various mathematicians. This is why in this book we also write about the people behind the results, mentioning their successes and sometimes their failures.

Finally, to help the reader get the big picture of how our understanding of the primes evolved over the years, we provide in Appendix A a time line of some key results on prime numbers.

Short biographies

The text is interspersed with short biographies of key players in the history of number theory. Our choice was subjective. Also, after some of these bios, we added anecdotes concerning these particular mathematicians. Our sources are essentially textbooks on the history of mathematics and we performed no additional fact-checking. In any event, we do hope that these bios and stories will contribute to humanizing mathematics, an aspect all too often neglected in many math books.

The plan of the monograph

This monograph is divided along five general themes:

- Part 1: Counting primes, the road to the prime number theorem
- Part 2: Counting primes, beyond the prime number theorem
- Part 3: Is it a prime?
- Part 4: Finding the prime factors of a given integer
- Part 5: Making good use of the primes and moving forward

Each of these five parts consists of "episodes", for a total of 37. These episodes are mostly presented in chronological order, which reflects how prime number theory progressed over the years. Of course, many episodes overlap in time and this is mostly because the various topics involving prime numbers are in constant evolution. Episode 36 is a kind of consolation prize. Indeed, through the first 35 episodes we visit numerous mysteries surrounding prime numbers some of which confirm our somewhat poor capabilities in factoring large integers. One can then rejoice in reading Episode 36, because in the end, as we will explain, our ignorance regarding the factorisation of large integers does serve us well and has in fact paved the way for the MIT mathematicians Ron Rivest, Adi Shamir and Leonard Adleman to create the first practical public-key cryptosystem, the *RSA algorithm*. This particular episode does indeed describe the fundamental role played by prime numbers in today's most secure encryption method. In a sense, it reinforces the idea that many areas of pure mathematics end up having some applications relevant to our everyday well-being, and prime number theory is no exception. The last episode is a preview of some of the features one can expect for the future life of primes.

Prerequisites

The reader is assumed to have some background in number theory, for instance to have attended an undergraduate course in number theory. Some knowledge of complex analysis could be useful if the reader wants to understand the analytic proof of the prime number theorem given in Episode 12 and truly appreciate the oscillation theorems presented in Episode 18. The episodes and subsections marked with a star (*) may require more knowledge than is normally covered at the undergraduate level. In any event, these particular segments may be skipped by the reader without impeding on his or her ability to comprehend other parts of the monograph. In order for the book to be as self-contained as possible, in Appendix C we added a list of basic results in number theory, algebra and analysis which may be helpful to the reader.

Problems

Each episode ends with a series of problems that should help the reader gain a better understanding of the theory. Any problem marked with a star (*) represents a real challenge as it may require advanced knowledge and can therefore be skipped. Those problems marked with two stars (**) are even more challenging. In Appendix B, for more than half of the problems we provide either a hint, a partial or complete solution. We made an effort to lay out the solutions for the most difficult ones.

Computer programs

We think that to really appreciate prime number theory, especially when it comes to identifying those large numbers with a given property or simply to find a counterexample to some statement, a computing software will come in handy. Each mathematician has his or her favorite. We like to work with MATHEMATICA. This is why, at times, the reader will encounter some short programs written with MATHEMATICA. Since its language is fairly intuitive, the reader not familiar with it will nevertheless most likely be able to understand the general meaning of the

few lines of programming offered and then manage to reach the same goal with his or her own favorite software.

Acknowledgments

In writing this book, we benefited from the precious advice and insight of several colleagues and students. Our first thanks go to Florian Luca who strongly encouraged the first author to go ahead with this project when they were both teaching at AIMS Ghana in March 2016. We wish to thank Imre Kátai and Oleksiy Klurman for suggesting new problems which appear throughout this book. We are also grateful to David Ayotte, Zita De Koninck, Fenomila Dionah Naivoarilala, Vincent Ouellet and Arthur Razafindrasoanaivolala for raising several questions which greatly improved our manuscript. Special thanks to our colleague Bernard Hodgson who revised all the short biographies and shared precious advice. We are also obliged to our colleague Claude Levesque who pointed out several errors in an earlier version and provided several constructive comments. Our thanks also go to the various anonymous reviewers whose comments greatly helped improve the quality of our presentation.

Jean-Marie De Koninck

Nicolas Doyon