An Introduction to Number Theory with Cryptography

Authors: James S. Kraft, Lawrence C. Washington

Reviewer: Capi Corrales Rodrigáñez, Department of Algebra, Mathematics, UCM, Madrid

"There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definition and role as the building blocks of the natural numbers, the prime numbers grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision." (Don Zagier, *The first 50 million prime numbers.* The new Mathematical Intelligencer, Vol. 0, August 1977, 1-19.)

"No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years." (G.H. Hardy (1877-1947), *A Mathematicians Apology*, Section 28.)

This two quotes, the only ones in its introduction, frame nicely much of what can be found in the book under review. Early cryptography was synonymous of encryption, the process of converting messages into a form unreadable by anyone except the intended recipient. For centuries, people have sent secret information by various means. In ancient China, messages were often transformed into ideographs for privacy. Indian ciphers consisted mostly of simple alphabetic substitutions often based on phonetics. The Spartans wrapped a thin sheet of papyrus around a staff, wrote the message down the length of the staff and unwrapped the papyrus; in order to read the message, the papyrus had to be wrapped around a staff of equal diameter. And Julius Caesar used a system of cryptography which shifted each letter two places further through the alphabet. These are a few examples of *encryption*. Modern cryptography, on the other hand, though still keeping as basic purpose the protection of communications, includes many related applications such as sender/receiver identity authentication, or digital signatures. The breaking point took place in the 1970s, when number theoretical tools from modular arithmetic, the study of primes and prime factorization, became fundamental ingredients in many cryptographic systems. For example, in 1976 W Diffie and M. Hellman introduced the concept of public key cryptography, based in modular arithmetic, and also gave a key establishment of protocol that uses large primes. A year later, R. Rivest, A. Shamir and L. Adleman implemented the public key concept in what is known as the RSA cryptosystem; it uses large primes, and its security is tied to the difficulty of factoring large integers. As a consequence, in the mid-1970s, cryptography popularized the search for primes and research in topics such as factorization and the two aspects of the distribution of primes described in Zagier's quote. And it also changed the standard view so far held of number theory. Thanks to cryptography, Hardy's statement is no longer true. In the last decades, the ideas developed in number theory to solve cryptographic problems have inspired many related applications.

Much of Kraft and Washington's volume is dedicated to the study of integers. Their basic properties are introduced in the first part of the book, namely divisibility of integers (introduced in chapter 1), unique factorization of integers into products of primes (chapters 2 and 3) and congruences, the partitions obtained when integers are classified according to the remainder that they produced when divided by a fixed number (chapter 4). These basic properties are all that is needed for the construction of the cryptographic systems studied in chapter 5: shift and affine ciphers, secret sharing and RSA. A deeper study of congruences, also known as modular arithmetic (polynomial congruences in chapter 6 and orders and primitive roots in chapter 7), soon leads to the search for effective algorithms that will make computations feasible. The security of many codes

relies on the fact that the computations necessary to break them could theoretically be done, but they would require so much time that in practice the codes can be assumed safe. These computational problems produced much beautiful mathematics which, in turn, inspired new computational developments. An example is the baby step-giant step method developed by D. Shanks ([**?**]), one of the algorithms explained in chapter 7. These algorithms, together with the material exposed previously, suffice for the construction of the cryptographic applications explained in the next chapter: the Diffie-Helman key exchange, coin flipping over the telephone, mental poker, the ElGamal public key crypto system and digital signatures.

The second part of the book starts with a classical result in number theory: the law of quadratic reciprocity.

"The Law of Quadratic Reciprocity is one of the high points in number theory. It was conjectures by Euler (1744) and Legendre (1785). In 1796, when he was 18 years old, Gauss gave the first proof. Gauss published six proofs during his lifetime, and two more where found in his unpublished manuscripts. Attempts to generalize Quadratic Reciprocity inspired the development of algebraic number theory in the 1800s and 1900s, and greatly influenced modern areas of research such as elliptic curves and modular forms from the 1900s up to the present. Quadratic Reciprocity is the deepest theorem that we will meet in this book." (J. Kraft, L. Washington, [**?**], p. 266.)

This law, its proof and its applications, form the core of chapter 10. The popularity of cryptographic algorithms using primes, has brought to the front line two fundamental computational problems of number theory: finding large primes (and, so, primality testing) and factoring composite numbers. This two problems, related but intrinsically different, as well as some of the algorithms most commonly used to face them –such as the Pockington-Lehmer or the AKS Primality tests–, are discussed in chapter 10. The rest of the book is dedicated to the most computational aspects of other classical topics in number theory: the geometry of numbers and its applications to writing integers as sums of squares and Pell's equation (Chapter 11), the arithmetic multiplicative functions (chapter 12), continued fractions and rational approximations (chapter 13), the arithmetic of Gaussian integers and quadratic fields and how they can be used to study properties of rational integers (chapters 14 and 15) and, finally, how techniques from calculus can help obtain information about how primes are distributed. The book ends with an Epilogue on Andrew Wiles' proof of Fermat's Last Theorem and an Appendix of supplementary topics. Unfortunately, in the volume we have in hands both sections have most of the pages blank and the reviewer has been unable to read them.

Despite this uncomfortable printing error, *An Introduction to Number Theory with Cryptography* is a highly recommended book both for students and for anyone, including professional mathematicians, who wants to learn about one of the nowadays most alive and exciting applications of mathematics. Undoubtly designed with a didactic purpose as well as for pleasure, the book is written in a down-to earth style, is mostly self sufficient and it is full of practical examples and useful exercises. This makes its reading as easy and comfortable as appealing, giving the reader the satisfaction of being able to understand and readily put to work some very beautiful and alive mathematics.

References

[1] J. Kraft, L. Washington, *An introduction to Number Theory with Cryptography*, CRC Press, 2014. ISBN-13 978-1-4822-1441-3.

[2] Daniel Shanks, *Class number, a theory of factorization, and genera*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969) Amer. Math. Soc., 1971, pp. 415-440.