PREFACE

In this book the author treats four fundamental and apparently simple problems. They are: the number of primes below a given limit, the approximate number of primes, the recognition of prime numbers and the factorization of large numbers. A chapter on the details of the distribution of the primes is included as well as a short description of a recent application of prime numbers, the so-called RSA public-key cryptosystem. The author is also giving explicit algorithms and computer programs. Whilst not claiming completeness, the author has tried to give all important results known, including the latest discoveries. The use of computers has in this area promoted a development which has enormously enlarged the wealth of results known and that has made many older works and tables obsolete.

As is often the case in number theory, the problems posed are easy to understand but the solutions are theoretically advanced. Since this text is aimed at the mathematically inclined layman, as well as at the more advanced student, not all of the proofs of the results given in this book are shown. Bibliographical references in these cases serve those readers who wish to probe deeper. References to recent original works are also given for those who wish to pursue some topic further.

Since number theory is seldom taught in basic mathematics courses, the author has appended six sections containing all the algebra and number theory required for the main body of the book. There are also two sections on multiple precision computations and, finally, one section on Stieltjes integrals. This organization of the subject-matter has been chosen in order not to disrupt the reader's line of thought by long digressions into other areas. It is also the author's hope that the text, organized in this way, becomes more readable for specialists in the field. Any reader who gets stuck in the main text should first consult the appropriate appendix, and then try to continue.

The six chapters of the main text are quite independent of each other, and need not be read in order.

For those readers who have a computer (or even a programmable calculator) available, computer programs have been provided for many of the methods described. In order to achieve a wide understanding, these programs are written in the high-level programming language PASCAL. With this choice the author hopes that most readers will be able to translate the programs into the language of the computer they use with reasonable effort.

PREFACE

At the end of the book a large amount of results are collected in the form of tables, originating partly from the author's own work in this field. All tables have been verified and up-dated as far as possible. Also in connection with the tables, bibliographical references are given to recent or to more extensive work in the corresponding area.

The text is an up-dated version of an earlier book by the same author: "En bok om primtal," existing in Swedish only.

The author is very much indebted to Richard Brent, Arne Fransén, Gunnar Hellström, Hans Karlgren, D. H. Lehmer, Thorkil Naur, Andrzej Schinzel, Bob Vaughan and many others for their reading of the manuscript and for suggesting many improvements. Thanks are also due to Beatrice Frock for revising the English, and to the late Ken Clements for reading and correcting one of the last versions of the manuscript.

The author wishes you a pleasant reading!

Stockholm, February 1985

PREFACE TO THE SECOND EDITION

During the last ten years the science of computational number theory has seen great advances. Several important new methods have been introduced to recognize prime numbers and to factor composite integers. These advances have stimulated the author to add subsections on the applications of the elliptic curve method and on the number field sieve to the main text as well as two new appendices covering the basics of these new subjects.—Also, very many minor updatings and corrections of the text have been made.

The author wishes to express his thanks to the many readers who have written during the years and proposed improvements of the text. Special thanks are going to Richard Brent, François Morain, Peter Montgomery and in particular to Harvey Dubner and Wilfrid Keller, who all helped during various stages of the preparation of the new manuscript.

Stockholm, June 1994

http://www.springer.com/978-0-8176-8297-2

Prime Numbers and Computer Methods for Factorization

Riesel, H.

2012, XVIII, 464 p. 20 illus., Softcover
ISBN: 978-0-8176-8297-2
A product of Birkhäuser Basel