

Preface

Chinese Remainder Theorem, CRT, is one of the jewels of mathematics. It is a perfect combination of beauty and utility or, in the words of Horace, *omne tulit punctum qui miscuit utile dulci*. Known already for ages, CRT continues to present itself in new contexts and open vistas for new types of applications. So far, its usefulness has been obvious within the realm of “three C’s”. Computing was its original field of applications, and continues to be important as regards various aspects of algorithmics and modular computations. Theory of codes and cryptography are two more recent fields of application.

This book tells about CRT, its background and philosophy, history, generalizations and, most importantly, its applications. The book is self-contained. This means that no factual knowledge is assumed on the part of the reader. We even provide brief tutorials on relevant subjects, algebra and information theory. However, some mathematical maturity is surely a prerequisite, as our presentation is at an advanced undergraduate or beginning graduate level. We have tried to make the exposition innovative, many of the individual results being new.

A special course about CRT can be based on the book. The individual chapters are largely independent and, consequently, the book can be used as supplementary material for courses in algorithmics, coding theory, cryptography or the theory of computing. Of course, the book is also a reference for matters dealing with CRT.

Acknowledgements: We would like to thank the Academy of Finland, Chinese Academy of Science, and the Turku Centre for Computer Science (officially listed as one of the top twelve research centers in Finland) for providing us with excellent working conditions and financial support for our research. Special thanks are due to Elisa Mikkola for her assistance in several aspects of the project. Also we want to thank World Scientific, and especially Mr. Richard Lim, for good cooperation in this book project. We would also like to thank all members of our families for their support.

August 1996,

Cunsheng Ding Dingyi Pei Arto Salomaa