Review of the book

"Prime Numbers: A Computational Perspective"

Richard Crandall, Carl Pomerance

Springer, 2nd Edition, 2005

ISBN: 978-0387-25282-7

Dr Kian B Tay
Center for Strategic Infocomm Technologies

1 What the book is about

Number theory is known as the queen of math, and prime numbers are her beautiful building blocks, which occurs highly irregularly and yet "predictably", as spelt out by one of the most famous math breakthroughs, the PNT (Prime Number Theorem), which gives us an asymptotic estimate to the overall distribution of primes over a large interval! With the invention of public key cryptography like RSA and discrete log based cryptosystems, prime numbers are not just interesting in math but in cryptography and the reaal world applications of e-comerce. This book tells us many facts about prime numbers, how to recognise a number is prime efficiently, and how to factorise a number into primes quickly. It covers not just theoretical number theory but the computational aspects which is lacking in most number theory books.

2 What the book is like

One can hardly find a better duo to write such a book: Carl Pomerance and Richard Crandall. Pomerance was the discoverer of the quadratic sieve factoring algorithm, and he has won many awards on expository writing from MAA. Crandall (now deceased) was former chief cryptographer, Distinguished Scientist of Apple, Chief Scientist at NeXT and he had PhD in both math and physics! The book is painstakingly well written (it is enough just to take a look at how they explain the deepest math in computational number theory, which is the fastest factoring algorithm, aka Number Field Sieve) , and along the way interesting authoritative remarks are given at the appropriate places (see for example, page 37, where they stated the equivalence of PNT and the growth of Mertens Function; quote:

"*What a compelling notion, that the Mertens Function, which one might envision as something like a random wealk, with the Mobius mu contributing to the summation for M in something like the style of a random coin flip, should be so closely related to the Great Prime Number Theorem, and the Great Conjecture (Riemann Hypothesis) in this way!*"

The academic community has to really thank them for taking their precious time off their scientific research to educate us by writing this magnificent opus on number theory.

There are 9 chapters in this 600 page book with many subchapters:
The book starts with a 82 page story on Primes, followed by Number Theoretical tools (34 pp), Recognising primes and composites (56 pp), primality proving (52 pp), Exponential factoring algorithms (36 pp), sub-exponential factoring algorithms (58 pp), elliptic curve arithmetic (68 pp), the ubiquity of prime numbers (56 pp), fast algorithms for large integer arithmetic (98 pp) and a great compendium of references and an appendix on Pseudocode! To list down all the sub-chapters will be too long; those interested should take a look at the book website or google the book images for detailed contents.

Some highlights from the book:
It starts off with a paragraph or two on what the chpater is all about. Proofs are given most of the time. They really bother to explain in detail the difficult math in Number Field Sieve etc. Pseudocodes are given for the more important algorithms (complexity of the algorithms are there as well). As far as I can tell, all the algorithms are tabulated in a very clear display. This is most helpful to implementers. Many practical examples are also given. A list of problems is also there for exercise and experimentation. They have actively included the genesis of important results and the people who have found them-it makes this book a more interesting read!

This book is still fairly up to date as the second edition has only been published in 2005. There are hardly any new topic of interest that the team did not cover. Even the latest results on Implementation of elliptic curve factoring algorithm is there. A minor handicap is of course the fact that some important recent discoveries are not found in the book, such as the factoring of RSA-768, the various discrete log records the past 2 years by Joux, Granger and their teams. Also the famous theorem by Tom Zhang Yitang on Bounded gaps between primes is not there. Do check out the latest results on the web if you are working on any topic in this book.

3 What I like about this book

The typeface and the presentation are done professionally. Every page is interesting in some ways and the writing style is inviting.

What are the qualities of a great book on computational number theory? Is it readable and clear? Is it written by experts in the fields? Are all the important results listed? Are the references comprehensive? Are the topics chosen useful and important? Is the printing and layout clear for reading?

One would have to answer a resounding yes to all these questions. This book fulfills all these admirably. It will be extremely hard to come up with a better book on computational number theory, written by a better group of experts.

4 Possible Improvements

None really. The publisher only need to update the latest results for possible future editions at this time, and include new important topics as and when they arise.

5 Would you recommend this book?

A resounding YES. It is suitable for motivated math, computer science or engineering students and professionals. It is arguably the best book on computational number theory. It is certainly a valuable resource for mathematicians and cryptographers now and in the years to come.
I really love this book! Enough said.

The reviewer is a researcher in infocomm security with specialty in math and cryptography. He was formerly a professor in math.