Song Y. Yan

Number Theory for Computing

2nd Edition

计算数论

第2版

Springer-Verlag
世界图书出版公司

Song Y. Yan

Number Theory for Computing

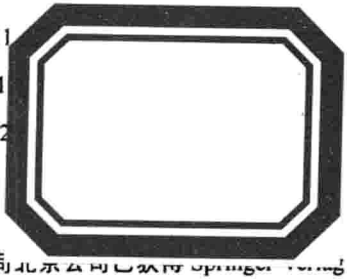
Second Edition

Foreword by Martin E. Hellman

With 26 Figures, 78 Images, and 33 Tables

Springer
世界图书出版公司

书　　名：Number Theory for Computing　2nd Edition
作　　者：Song Y. Yan
中 译 名：计算数论 第 2 版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
发　　行：世界图书出版公司北京公司 (北京朝内大街 137 号　100010)
联系电话：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开　　本：24 开　　印　张：19.5
出版年代：2004 年 11
书　　号：7-5062-71
版权登记：图字:01-2
定　　价：59.00 元



Song Y. Yan
Computer Science
Aston University
Birmingham B4 7ET
UK
s.yan@aston.ac.uk

ACM Computing Classification (1998): F.2.1, E.3-4, D.4.6, B.2.4, I.1.2

AMS Mathematics Subject Classification (1991): 11Axx, 11T71, 11Yxx, 11Dxx, 11Z05, 68Q25, 94A60

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Yan, Song Y.:
Number theory for computing: with 32 tables/Song Y. Yan. - 2. ed., rev. and extended. - Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan; Paris; Tokyo: Springer, 2002
ISBN 3-540-43072-5

ISBN 3-540-43072-5 Springer-Verlag Berlin Heidelber New York
ISBN 3-540-65472-0 Springer-Verlag Berlin Heidelberg New York (1st ed.)

Springer-Verlag Berlin Heidelberg New York,
a member of BertelsmannSpringer Science+Business Media GmbH
http://www.springer.de

Printed in Germany

Foreword

Modern cryptography depends heavily on number theory, with primality testing, factoring, discrete logarithms (indices), and elliptic curves being perhaps the most prominent subject areas. Since my own graduate study had emphasized probability theory, statistics, and real analysis, when I started working in cryptography around 1970, I found myself swimming in an unknown, murky sea. I thus know from personal experience how inaccessible number theory can be to the uninitiated. Thank you for your efforts to ease the transition for a new generation of cryptographers.

Thank you also for helping Ralph Merkle receive the credit he deserves. Diffie, Rivest, Shamir, Adleman and I had the good luck to get expedited review of our papers, so that they appeared before Merkle's seminal contribution. Your noting his early submission date and referring to what has come to be called "Diffie-Hellman key exchange" as it should, "Diffie-Hellman-Merkle key exchange", is greatly appreciated.

It has been gratifying to see how cryptography and number theory have helped each other over the last twenty-five years. Number theory has been the source of numerous clever ideas for implementing cryptographic systems and protocols while cryptography has been helpful in getting funding for this area which has sometimes been called "the queen of mathematics" because of its seeming lack of real world applications. Little did they know!

Stanford, 30 July 2001 Martin E. Hellman

Preface to the Second Edition

Number theory is an experimental science.

J. W. S. CASSELS (1922–)
Professor Emeritus of Mathematics, The University of Cambridge

If you teach a course on number theory nowadays, chances are it will generate more interest among computer science majors than among mathematics majors. Many will care little about integers that can be expressed as the sum of two squares. They will prefer to learn how Alice can send a message to Bob without fear of eavesdropper Eve deciphering it.

BRAIN E. BLANK, Professor of Mathematics
Washington University, St. Louis, Missouri

The success of the first edition of the book encouraged me to produce this second edition. I have taken this opportunity to provide proofs of many theorems, that had not been given in the first edition. Some additions and corrections have also been included.

Since the publication of the first edition, I have received many communications from readers all over the world. It is my great pleasure to thank the following people for their comments, corrections and encouragements: Prof. Jim Austin, Prof. Friedrich L. Bauer, Dr. Hassan Daghigh Dr. Deniz Deveci, Mr. Rich Fearn, Prof. Martin Hellman, Prof. Zixin Hou, Mr. Waseem Hussain, Dr. Gerard R. Maze, Dr. Paul Maguire, Dr. Helmut Meyn, Mr. Robert Pargeter, Mr. Mok-Kong Shen, Dr. Peter Shiu, Prof. Jonathan P. Sorenson, and Dr. David L. Stern. Special thanks must be given to Prof. Martin Hellman of Stanford University for writing the kind Foreword to this edition and also for his helpful advice and kind guidance, to Dr. Hans Wössner, Mr. Alfred Hofmann, Mrs. Ingeborg Mayer, Mrs. Ulrike Stricker, and Mr. Frank Holzwarth of Springer-Verlag for their kind help and encouragements during the preparation of this edition, and to Dr. Rodney Coleman, Prof. Glyn James, Mr. Alexandros Papanikolaou, and Mr. Robert Pargeter for proofreading the final draft. Finally, I would like to thank Prof. Shiing-Shen Chern,

Director Emeritus of the Mathematical Sciences Research Institute in Berkeley for his kind encouragements; this edition is dedicated to his 90th birthday!

Readers of the book are, of course, very welcome to communicate with the author either by ordinary mail or by e-mail to `s.yan@aston.ac.uk`, so that your corrections, comments and suggestions can be incorporated into a future edition.

Birmingham, February 2002 S. Y. Y.

Preface to the First Edition

Mathematicians do not study objects, but relations among objects; they are indifferent to the replacement of objects by others as long as relations do not change. Matter is not important, only form interests them.

HENRI POINCARÉ (1854–1912)

Computer scientists working on algorithms for factorization would be well advised to brush up on their number theory.

IAN STEWART
Geometry Finds Factor Fast
Nature, Vol. 325, 15 January 1987, page 199

The theory of numbers, in mathematics, is primarily the theory of the properties of integers (i.e., the whole numbers), particularly the positive integers. For example, Euclid proved 2000 years ago in his *Elements* that there exist infinitely many prime numbers. The subject had long been considered as the *purest* branch of mathematics, with very few applications to other areas. However, recent years have seen considerable increase in interest in several central topics of number theory, precisely because of their importance and applications in other areas, particularly in computing and information technology. Today, number theory has been applied to such diverse areas as physics, chemistry, acoustics, biology, computing, coding and cryptography, digital communications, graphics design, and even music and business[1]. In particular, congruence theory has been used in constructing perpetual calendars, scheduling round-robin tournaments, splicing telephone cables, devising systematic methods for storing computer files, constructing magic squares, generating random numbers, producing highly secure and reliable encryption schemes and even designing high-speed (residue) computers. It is specifically worthwhile pointing out that computers are basically finite machines; they

[1] In his paper [96] in the *International Business Week*, 20 June 1994, pp. 62–64, Fred Guterl wrote: "Number Theory, once the esoteric study of what happens when whole numbers are manipulated in various ways, is becoming a vital practical science that is helping solve tough business problems".

have finite storage, can only deal with numbers of some finite length and can only perform essentially finite steps of computation. Because of such limitations, congruence arithmetic is particularly useful in computer hardware and software design.

This book takes the reader on a journey, starting at elementary number theory, going through algorithmic and computational number theory, and finally finishing at applied number theory in computing science. It is divided into three distinct parts:

(1) Elementary Number Theory,

(2) Computational/Algorithmic Number Theory,

(3) Applied Number Theory in Computing and Cryptography.

The first part is mainly concerned with the basic concepts and results of divisibility theory, congruence theory, continued fractions, Diophantine equations and elliptic curves. A novel feature of this part is that it contains an account of elliptic curves, which is not normally provided by an elementary number theory book. The second part provides a brief introduction to the basic concepts of algorithms and complexity, and introduces some important and widely used algorithms in computational number theory, particularly those for primality testing, integer factorization, discrete logarithms, and elliptic curve discrete logarithms. An important feature of this part is that it contains a section on quantum algorithms for integer factorization and discrete logarithms, which cannot be easily found, so far, in other texts on computational/algorithmic number theory. This part finishes with sections on algorithms for computing $\pi(x)$, for finding amicable pairs, for verifying Goldbach's conjecture, and for finding perfect and amicable numbers. The third part of the book discusses some novel applications of elementary and computational number theory in computing and information technology, particularly in cryptography and information security; it covers a wide range of topics such as secure communications, information systems security, computer organisations and design, error detections and corrections, hash function design, and random number generation. Throughout the book we follow the style "Definition-Theorem-Algorithm-Example" to present our material, rather than the traditional Hardy–Wright "Definition-Theorem-Proof" style [100], although we do give proofs to most of the theorems. We believe this is the most suitable way to present mathematical material to computing professionals. As Donald Knuth [121] pointed out in 1974; "It has often been said that a person does not really understand something until he teaches it to someone else. Actually a person does not really understand something until he can teach it to a computer." The author strongly recommends readers to implement all the algorithms and methods introduced in this book on a computer using a mathematics (computer algebra) system such as Maple in order to get a better understanding of the ideas behind the algorithms and

methods. A small number of exercises is also provided in some sections, and it is worthwhile trying all of them.

The book is intended to be self-contained with no previous knowledge of number theory and abstract algebra assumed, although some familiarity with first-year undergraduate mathematics will be helpful. The book is suitable either as a text for an undergraduate/postgraduate course in *Number Theory/Mathematics for Computing/Cryptography*, or as a basic reference researchers in the field.

Acknowledgements

I started to write this book in 1990 when I was a lecturer in the School of Mathematical and Information Sciences at La Trobe University, Australia. I completed the book when I was at the University of York and finalized it at Coventry and Aston Universities, all in England. I am very grateful to Prof. Bertram Mond and Dr. John Zeleznikow of the School of Mathematical and Information Sciences at La Trobe University, Dr. Terence Jackson of the Department of Mathematics and Prof. Jim Austin of the Department of Computer Science at the University of York, Prof. Glyn James, Mr. Brian Aspinall and Mr. Eric Tatham of the School of Mathematical and Information Sciences at Coventry University, and Prof. David Lowe and Dr. Ted Elsworth of Computer Science and Applied Mathematics at Aston University in Birmingham for their many fruitful discussions, kind encouragement and generous support. Special thanks must be given to Dr. Hans Wössner and Mr. Andrew Ross at Springer-Verlag Berlin/Heidelberg and the referees of Springer-Verlag, for their comments, corrections and suggestions. During the long period of the preparation of the book, I also got much help in one way or another from, whether they are aware of it or not, Prof. Eric Bach of the University of Wisconsin at Madison, Prof. Jim Davenport of the University of Bath, Prof. Richard Guy of the University of Calgary, Prof. Martin Hellman of Stanford University, Dr. David Johnson of AT&T Bell Laboratories, Prof. S. Lakshmivarahan of the University of Oklahoma, Dr. Ajie Lenstra of Bell Communication Research, Prof. Hendrik Lenstra Jr. of the University of California at Berkeley, Prof. Roger Needham and Dr. Richard Pinch of the University of Cambridge, Dr. Peter Pleasants of the University of the South Pacific (Fiji), Prof. Carl Pomerance of the University of Georgia, Dr. Herman te Riele of the Centre for Mathematics and Computer Science (CWI), Amsterdam, and Prof. Hugh William of the University of Manitoba. Finally, I would like to thank Mr. William Bloodworth (Dallas, Texas), Dr. John Cosgrave (St. Patrick's College, Dublin), Dr. Gavin Doherty (Rutherford Appleton Laboratory, Oxfordshire), Mr. Robert Pargeter (Tiverton, Devon), Mr. Alexandros Papanikolaou (Aston University, Birmingham),

and particularly Prof. Richard Brent (Oxford University Computing Laboratory), Dr. Rodney Coleman (Université Joseph Fourier, Grenoble) and Prof. Glyn James (Coventry University) for reading the various versions of the book. As communicated by Dr. Hans Wössner: nothing is perfect and nobody is perfect. This book and the author are no exception. Any comments, corrections and suggestions from readers of the book are especially very welcome and can be sent to the author either by ordinary mail or by e-mail to s.yan@aston.ac.uk.

Birmingham, February 2000 S. Y. Y.

Notation

All notation should be as simple as the nature of the operations to which it is applied.

CHARLES BABBAGE (1791–1871)

Notation	Explanation
$\mathbb{N}$	set of natural numbers: $\mathbb{N} = \{1, 2, 3, \cdots\}$
$\mathbb{Z}$	set of integers (whole numbers): $\mathbb{Z} = \{0, \pm n : n \in \mathbb{N}\}$
$\mathbb{Z}^+$	set of positive integers: $\mathbb{Z}^+ = \mathbb{N}$
$\mathbb{Z}_{>1}$	set of positive integers greater than 1: $\mathbb{Z}_{>1} = \{n : n \in \mathbb{Z} \text{ and } n > 1\}$
$\mathbb{Q}$	set of rational numbers: $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$
$\mathbb{R}$	set of real numbers: $\mathbb{R} = \{n + 0.d_1 d_2 d_3 \cdots : n \in \mathbb{Z},\ d_i \in \{0, 1, \cdots, 9\}$ and no infinite sequence of 9's appears$\}$
$\mathbb{C}$	set of complex numbers: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\}$
$\mathbb{Z}/n\mathbb{Z}$	also denoted by $\mathbb{Z}_n$, residue classes modulo n; a ring of integers; a field if n is prime
$(\mathbb{Z}/n\mathbb{Z})^*$	multiplicative group; the elements of this group are the elements in $\mathbb{Z}/n\mathbb{Z}$ that are relatively prime to n: $(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} :\ \gcd(a, n) = 1\}$.
$\mathbb{F}_p$	finite field with p elements, where p is a prime number
$\mathbb{F}_q$	finite field with $q = p^k$ a prime power
$\mathcal{K}$	(arbitrary) field
$\mathcal{R}$	ring

$\mathcal{G}$	group
$\lvert\mathcal{G}\rvert$	order of group $\mathcal{G}$
B_n	Bernoulli numbers: $\binom{n+1}{1} B_n + \cdots + \binom{n+1}{n} B_1 + B_0 = 0$
F_n	Fermat numbers: $F_n = 2^{2^n} + 1,\ n \geq 0$
M_p	Mersenne primes: $M_p = 2^p - 1$ is prime whenever p is prime
$\sqrt{x}$	square root of x
$\sqrt[k]{x}$	kth root of x
$\sim$	asymptotic equality
$\approx$	approximate equality
∞	infinity
$\Longrightarrow$	implication
$\Longleftrightarrow$	equivalence
$\square$	blank symbol; end of proof
$\sqcup$	space
Prob	probability measure
$\lvert S\rvert$	cardinality of set S
$\in$	member of
$\subset$	proper subset
$\subseteq$	subset
$\star, *$	binary operations
$\oplus$	binary operation (addition); exclusive or (XOR)
$\odot$	binary operation (multiplication)
$f(x) \sim g(x)$	$f(x)$ and $g(x)$ are asymptotically equal
$(\mathcal{G}, *) \cong (\mathcal{H}, \star)$	$(\mathcal{G}, *)$ and $(\mathcal{H}, \star)$ are isomorphic
$\perp$	undefined
e_k	encryption key
d_k	decryption key
$E_{e_k}(M)$	encryption process $C = E_{e_k}(M)$, where M is the plaintext
$D_{d_k}(C)$	decryption process $M = D_{d_k}(C)$, where C is the ciphertext

$f(x)$	function of x
f^{-1}	inverse of f
$\binom{n}{i}$	binomial coefficient
$\int$	integration
$\mathrm{Li}(x)$	logarithmic integral: $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$
$\sum_{i=1}^{n} x_i$	sum: $x_1 + x_2 + \cdots + x_n$
$\prod_{i=1}^{n} x_i$	product: $x_1 x_2 \cdots x_n$
$n!$	factorial: $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$
x^k	x to the power k
kP	$kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ summands}}$, where P is a point (x, y) on an elliptic curve $E: \; y^2 = x^3 + ax + b$
$\mathcal{O}_E$	the point at infinity on an elliptic curve E over a field
e	the transcendental number $e = \sum_{n \geq 0} \frac{1}{n!} \approx 2.7182818$
$\log_b x$	logarithm of x to the base b ($b \neq 1$): $x = b^{\log_b x}$
$\log x$	binary logarithm: $\log_2 x$
$\ln x$	natural logarithm: $\log_e x$
$\exp(x)$	exponential of x: $e^x = \sum_{n \geq 0} \frac{x^n}{n!}$
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$p^\alpha \mid\mid n$	$p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$
$\gcd(a, b)$	greatest common divisor of (a, b)
$\mathrm{lcm}(a, b)$	least common multiple of (a, b)
$\lfloor x \rfloor$	the greatest integer less than or equal to x
$\lceil x \rceil$	the least integer greater than or equal to x
x mod n	remainder: $x - n \left\lfloor \frac{x}{n} \right\rfloor$
$x = y \bmod n$	x is equal to y reduced to modulo n
$x \equiv y \pmod{n}$	x is congruent to y modulo n
$x \not\equiv y \pmod{n}$	x is not congruent to y modulo n

$[a]_n$	residue class of a modulo n
$+_n$	addition modulo n
$-_n$	subtraction modulo n
$\cdot_n$	multiplication modulo n
$x^k \bmod n$	x to the power k modulo n
$kP \bmod n$	kP modulo n
$\operatorname{ord}_n(a)$	order of an integer a modulo n; also denoted by $\operatorname{ord}(a, n)$
$\operatorname{ind}_{g,n} a$	index of a to the base g modulo n; also denoted by $\operatorname{ind}_g a$ whenever n is fixed
$\pi(x)$	number of primes less than or equal to x: $\pi(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} 1$
$\tau(n)$	number of positive divisors of n: $\tau(n) = \sum_{d \mid n} 1$
$\sigma(n)$	sum of positive divisors of n: $\sigma(n) = \sum_{d \mid n} d$
$s(n)$	sum of proper divisors of n: $s(n) = \sigma(n) - n$
$\phi(n)$	Euler's totient function: $\phi(n) = \sum_{\substack{0 \le k < n \\ \gcd(k,n)=1}} 1$
$\lambda(n)$	Carmichael's function: $\lambda(n) = \operatorname{lcm}(\lambda(p_1^{\alpha_1})\lambda(p_2^{\alpha_2}) \cdots \lambda(p_k^{\alpha_k}))$ if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$
$\mu(n)$	Möbius function
$\zeta(s)$	Riemann zeta-function: $\zeta(s) = \prod_{n=1}^{\infty} \frac{1}{n^s}$, where s is a complex variable
$\left(\frac{a}{p}\right)$	Legendre symbol, where p is prime
$\left(\frac{a}{n}\right)$	Jacobi symbol, where n is composite
Q_n	set of all quadratic residues of n
$\overline{Q}_n$	set of all quadratic nonresidues of n
J_n	$J_n = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) = 1\right\}$
$\tilde{Q}_n$	set of all pseudosquares of n: $\tilde{Q}_n = J_n - Q_n$
$K(k)_n$	set of all kth power residues of n, where $k \ge 2$
$\overline{K(k)}_n$	set of all kth power nonresidues of n, where $k \ge 2$

$[q_0, q_1, q_2, \cdots, q_n]$	finite simple continued fraction
$C_k = \frac{P_k}{Q_k}$	k-th convergent of a continued fraction
$[q_0, q_1, q_2, \cdots]$	infinite simple continued fraction
$[q_0, q_1, \cdots, q_k, \overline{q_{k+1}, q_{k+2}, \cdots, q_{k+m}}]$	periodic simple continued fraction
$\mathcal{P}$	class of problems solvable in deterministic polynomial time
$\mathcal{NP}$	class of problems solvable in nondeterministic polynomial time
$\mathcal{RP}$	class of problems solvable in random polynomial time with one-sided errors
$\mathcal{BPP}$	class of problems solvable in random polynomial time with two-sided errors
$\mathcal{ZPP}$	class of problems solvable in random polynomial time with zero errors
$\mathcal{O}(\cdot)$	upper bound: $f(n) = \mathcal{O}(g(n))$ if there exists *some* constant $c > 0$ such that $f(n) \leq c \cdot g(n)$
$o(\cdot)$	upper bound that is not asymptotically tight: $f(n) = \mathcal{O}(g(n))$, $\forall c > 0$ such that $f(n) < c \cdot g(n)$
$\Omega(\cdot)$	low bound: $f(n) = \Omega(g(n))$ if there exists a constant c such that $f(n) \geq \frac{1}{c} \cdot g(n)$
$\Theta(\cdot)$	tight bound: $f(n) = \Theta(n)$ if $f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n))$
$\mathcal{O}(N^k)$	polynomial-time complexity measured in terms of arithmetic operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^k\right)$	polynomial-time complexity measured in terms of bit operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^{c \log N}\right)$	superpolynomial complexity, where $c > 0$ is a constant
$\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right)$	subexponential complexity, $\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right) = \mathcal{O}\left(N^{c\sqrt{\log\log N / \log N}}\right)$
$\mathcal{O}(\exp(x))$	exponential complexity, sometimes denoted by $\mathcal{O}(e^x)$
$\mathcal{O}(N^\epsilon)$	exponential complexity measured in terms of bit operations; $\mathcal{O}(N^\epsilon) = \mathcal{O}\left(2^{\epsilon \log N}\right)$, where $\epsilon > 0$ is a constant
CFRAC	Continued FRACtion method (for factoring)
ECM	Elliptic Curve Method (for factoring)

NFS	Number Field Sieve (for factoring)
QS/MPQS	Quadratic Sieve/Multiple Polynomial Quadratic Sieve (for factoring)
ECPP	Elliptic Curve Primality Proving
DES	Data Encryption Standard
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
RSA	Rivest-Shamir-Adleman
WWW	World Wide Web