

# Contents

<b>Preface</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>ix</b>
<b>Guiding the Reader</b>	<b>xv</b>
<b>Index of Notations</b>	<b>xvii</b>
<b>Introduction</b>	<b>1</b>
<b>1 How Many Prime Numbers Are There?</b>	<b>3</b>
I    Euclid's Proof . . . . .	3
II   Goldbach Did It Too! . . . . .	6
III  Euler's Proof . . . . .	8
IV  Thue's Proof . . . . .	9
V    Three Forgotten Proofs . . . . .	10
A    Perott's Proof . . . . .	10
B    Auric's Proof . . . . .	11
C    Métrod's Proof . . . . .	11
VI  Washington's Proof . . . . .	11
VII Furstenberg's Proof . . . . .	12
<b>2 How to Recognize Whether a Natural Number is a Prime</b>	<b>15</b>
I    The Sieve of Eratosthenes . . . . .	16

II	Some Fundamental Theorems on Congruences . . . . .	17
A	Fermat's Little Theorem and Primitive Roots Modulo a Prime . . . . .	17
B	The Theorem of Wilson . . . . .	21
C	The Properties of Giuga and of Wolstenholme . . . . .	21
D	The Power of a Prime Dividing a Factorial . . . . .	24
E	The Chinese Remainder Theorem . . . . .	26
F	Euler's Function . . . . .	28
G	Sequences of Binomials . . . . .	33
H	Quadratic Residues . . . . .	37
III	Classical Primality Tests Based on Congruences . . . . .	39
IV	Lucas Sequences . . . . .	44
V	Primality Tests Based on Lucas Sequences . . . . .	63
VI	Fermat Numbers . . . . .	70
VII	Mersenne Numbers . . . . .	75
VIII	Pseudoprimes . . . . .	88
A	Pseudoprimes in Base 2 ( $\text{psp}$ ) . . . . .	88
B	Pseudoprimes in Base $a$ ( $\text{psp}(a)$ ) . . . . .	92
C	Euler Pseudoprimes in Base $a$ ( $\text{epsp}(a)$ ) . . . . .	95
D	Strong Pseudoprimes in Base $a$ ( $\text{spsp}(a)$ ) . . . . .	96
IX	Carmichael Numbers . . . . .	100
X	Lucas Pseudoprimes . . . . .	103
A	Fibonacci Pseudoprimes . . . . .	104
B	Lucas Pseudoprimes ( $\text{lpsp}(P, Q)$ ) . . . . .	106
C	Euler-Lucas Pseudoprimes ( $\text{elpsp}(P, Q)$ ) and Strong Lucas Pseudoprimes ( $\text{slpsp}(P, Q)$ ) . . . . .	106
D	Carmichael–Lucas Numbers . . . . .	108
XI	Primality Testing and Factorization . . . . .	109
A	The Cost of Testing . . . . .	110
B	More Primality Tests . . . . .	111
C	Titanic and Curious Primes . . . . .	119
D	Factorization . . . . .	122
E	Public Key Cryptography . . . . .	126
<b>3</b>	<b>Are There Functions Defining Prime Numbers?</b>	<b>131</b>
I	Functions Satisfying Condition (a) . . . . .	131
II	Functions Satisfying Condition (b) . . . . .	137
III	Prime-Producing Polynomials . . . . .	138
A	Prime Values of Linear Polynomials . . . . .	139

	B	On Quadratic Fields . . . . .	140
	C	Prime-Producing Quadratic Polynomials . . . .	144
	D	The Prime Values and Prime Factors Races . .	148
IV		Functions Satisfying Condition (c) . . . . .	151
<b>4</b>		<b>How Are the Prime Numbers Distributed?</b>	<b>157</b>
I		The Function $\pi(x)$ . . . . .	158
	A	History Unfolding . . . . .	159
	B	Sums Involving the Möbius Function . . . . .	172
	C	Tables of Primes . . . . .	173
	D	The Exact Value of $\pi(x)$ and Comparison with $x/\log x$ , $\text{Li}(x)$ , and $R(x)$ . . . . .	174
	E	The Nontrivial Zeros of $\zeta(s)$ . . . . .	177
	F	Zero-Free Regions for $\zeta(s)$ and the Error Term in the Prime Number Theorem . . . . .	180
	G	Some Properties of $\pi(x)$ . . . . .	181
	H	The Distribution of Values of Euler's Function	183
II		The $n$ th Prime and Gaps Between Primes . . . . .	184
	A	The $n$ th Prime . . . . .	185
	B	Gaps Between Primes . . . . .	186
III		Twin Primes . . . . .	192
IV		Prime $k$ -Tuplets . . . . .	197
V		Primes in Arithmetic Progression . . . . .	204
	A	There Are Infinitely Many! . . . . .	204
	B	The Smallest Prime in an Arithmetic Progression . . . . .	207
	C	Strings of Primes in Arithmetic Progression . .	209
VI		Goldbach's Famous Conjecture . . . . .	211
VII		The Distribution of Pseudoprimes and of Carmichael Numbers . . . . .	216
	A	Distribution of Pseudoprimes . . . . .	216
	B	Distribution of Carmichael Numbers . . . . .	218
	C	Distribution of Lucas Pseudoprimes . . . . .	220
<b>5</b>		<b>Which Special Kinds of Primes Have Been Considered?</b>	<b>223</b>
I		Regular Primes . . . . .	223
II		Sophie Germain Primes . . . . .	227
III		Wieferich Primes . . . . .	230
IV		Wilson Primes . . . . .	234

V	Repunits . . . . .	235
VI	Numbers $k \times b^n \pm 1$ . . . . .	237
VII	Primes and Second-Order Linear Recurrence Sequences . . . . .	243
<b>6</b>	<b>Heuristic and Probabilistic Results About Prime Numbers</b>	<b>249</b>
I	Prime Values of Linear Polynomials . . . . .	250
II	Prime Values of Polynomials of Arbitrary Degree . . .	253
III	Polynomials with Many Successive Composite Values .	261
IV	Partitio Numerorum . . . . .	263
	<b>Appendix 1</b>	<b>269</b>
	<b>Appendix 2</b>	<b>275</b>
	<b>Conclusion</b>	<b>279</b>
	<b>Bibliography</b>	<b>281</b>
	<b>Web Site Sources</b>	<b>325</b>
	<b>Primes up to 10,000</b>	<b>327</b>
	<b>Index of Tables</b>	<b>331</b>
	<b>Index of Records</b>	<b>333</b>
	<b>Index of Names</b>	<b>335</b>
	<b>Subject Index</b>	<b>349</b>



<http://www.springer.com/978-0-387-20169-6>

The Little Book of Bigger Primes

Ribenboim, P.

2004, XXIII, 356 p., Softcover

ISBN: 978-0-387-20169-6