

The **New** Book of Prime Number Records

Springer Science+Business Media, LLC

Paulo Ribenboim

The **New** Book of Prime Number Records



Springer

Paulo Ribenboim
Department of Mathematics
and Statistics
Queen's University
Kingston, Ontario
K7L 3N6 Canada

Mathematics Subject Classification (1991): 11A41, 11B39, 11A51

Library of Congress Cataloging-in-Publication Data

Ribenboim, Paulo.

The new book of prime number records/Paulo Ribenboim. — 3rd ed.
p. cm.

Rev. ed. of: The book of prime number records. 2nd ed. c1989.

Includes bibliographical references and index.

ISBN 978-1-4612-6892-5 ISBN 978-1-4612-0759-7 (eBook)

DOI 10.1007/978-1-4612-0759-7

1. Numbers, Prime. I. Ribenboim, Paulo. Book of prime number
records. II. Title.

QA246.R47 1995

512'.72—dc20

95-5441

Printed on acid-free paper.

© 1988, 1989, 1996 Springer Science+Business Media New York

Originally published by Springer-Verlag New York, Inc in 1988, 1989, 1996

Softcover reprint of the hardcover 3rd edition 1988, 1989, 1996

All rights reserved. This work may not be translated or copied in whole or in part without
the written permission of the publisher Springer Science+Business Media, LLC,

except for brief excerpts in connection with reviews or scholarly

analysis. Use in connection with any form of information storage and retrieval, electronic
adaptation, computer software, or by similar or dissimilar methodology now known or here-
after developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if
the former are not especially identified, is not to be taken as a sign that such names, as under-
stood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by
anyone.

Production coordinated by Brian Howe and managed by Francine McNeill; manufacturing
supervised by Joe Quatela.

Typeset by Asco Trade Typesetting Ltd, Hong Kong.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4612-6892-5

Narrow road to
a far province.

Bashō

My Numbers Are My Happiness:

1. Huguette
2. Serge
3. Eric
4. Suzanne
5. Kelly
6. Katy
7. Erica
8. Eric

Not forgetting

0. Paulo, who counts the empty set \emptyset
and $\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$

Preface

This text originated as a lecture delivered November 20, 1984, at Queen's University, in the undergraduate colloquium series.

In another colloquium lecture, my colleague Morris Orzech, who had consulted the latest edition of the *Guinness Book of Records*, reminded me very gently that the most “innumerate” people of the world are of a certain tribe in Mato Grosso, Brazil. They do not even have a word to express the number “two” or the concept of plurality. “Yes, Morris, I’m from Brazil, but my book will contain numbers different from ‘one.’”

He added that the most boring 800-page book is by two Japanese mathematicians (whom I’ll not name) and consists of about 16 million decimal digits of the number π .

“I assure you, Morris, that in spite of the beauty of the apparent randomness of the decimal digits of π , I’ll be sure that my text will include also some words.”

And then I proceeded putting together the magic combination of words and numbers, which became *The Book of Prime Number Records*. If you have seen it, only extreme curiosity could impel you to have this one in your hands.

The New Book of Prime Number Records differs little from its predecessor in the general planning. But it contains new sections and updated records.

It has been comforting to learn about the countless computers (machines and men), grinding without stop, so that more lines with new large numbers could be added, bringing despair for the printers and proofreaders.

To give the tone, I begin with a probable new record:

RECORD

The fastest selling book on prime number records is. . . .

You may start reading it!

Kingston, Ontario, Canada

PAULO RIBENBOIM

Contents

| | |
|--|-------|
| Preface | ix |
| Guiding the Reader | xv |
| Index of Notations | xvii |
| Introduction | 1 |
| CHAPTER 1 | |
| How Many Prime Numbers Are There? | 3 |
| I. Euclid's Proof | 3 |
| II. Goldbach Did It Too! | 4 |
| III. Euler's Proof | 6 |
| IV. Thue's Proof | 7 |
| V. Three Forgotten Proofs | 8 |
| A. Perott's Proof | 8 |
| B. Auric's Proof | 9 |
| C. Métrod's Proof | 9 |
| VI. Washington's Proof | 9 |
| VII. Fürstenberg's Proof | 10 |
| VIII. Euclidean Sequences | 11 |
| IX. Generation of Infinite Sequences of Pairwise Relatively Prime Integers | 17 |
| CHAPTER 2 | |
| How to Recognize Whether a Natural Number Is a Prime | 19 |
| I. The Sieve of Eratosthenes | 20 |
| II. Some Fundamental Theorems on Congruences | 21 |
| A. Fermat's Little Theorem and Primitive Roots Modulo a Prime | 22 |
| B. The Theorem of Wilson | 25 |
| C. The Properties of Giuga, Wolstenholme, and Mann and Shanks | 28 |
| D. The Power of a Prime Dividing a Factorial | 30 |
| E. The Chinese Remainder Theorem | 33 |
| F. Euler's Function | 34 |
| G. Sequences of Binomials | 42 |
| H. Quadratic Residues | 46 |
| III. Classical Primality Tests Based on Congruences | 48 |
| IV. Lucas Sequences | 53 |
| V. Primality Tests Based on Lucas Sequences | 74 |
| VI. Fermat Numbers | 83 |

| | |
|--|-----|
| VII. Mersenne Numbers | 90 |
| VIII. Pseudoprimes | 103 |
| A. Pseudoprimes in Base 2 (psp) | 105 |
| B. Pseudoprimes in Base a (psp(a)) | 108 |
| C. Euler Pseudoprimes in Base a (epsp(a)) | 112 |
| D. Strong Pseudoprimes in Base a (spsp(a)) | 113 |
| E. Somer Pseudoprimes | 117 |
| IX. Carmichael Numbers | 118 |
| X. Lucas Pseudoprimes | 126 |
| A. Fibonacci Pseudoprimes | 127 |
| B. Lucas Pseudoprimes (lpsp(P, Q)) | 129 |
| C. Euler–Lucas Pseudoprimes (elpsp(P, Q)) and Strong Lucas Pseudoprimes (slpsp(P, Q)) | 130 |
| D. Somer–Lucas Pseudoprimes | 131 |
| E. Carmichael–Lucas Numbers | 132 |
| XI. Primality Testing and Large Primes | 135 |
| A. The Cost of Testing | 136 |
| B. More Primality Tests | 139 |
| C. Primality Certification | 153 |
| D. Fast Generation of Large Primes | 156 |
| E. Titanic Primes | 157 |
| F. Curious Primes | 159 |
| XII. Factorization and Public Key Cryptography | 162 |
| A. Factorization of Large Composite Integers | 163 |
| B. Public Key Cryptography | 172 |
| CHAPTER 3 | |
| Are There Functions Defining Prime Numbers? | 179 |
| I. Functions Satisfying Condition (a) | 179 |
| II. Functions Satisfying Condition (b) | 186 |
| III. Functions Satisfying Condition (c) | 187 |
| IV. Prime-Producing Polynomials | 196 |
| A. Surveying the Problems | 196 |
| B. Polynomials with Many Initial Prime Absolute Values | 197 |
| C. The Prime-Producing Polynomials Races | 203 |
| D. Primes of the Form $m^2 + 1$ | 206 |
| CHAPTER 4 | |
| How Are the Prime Numbers Distributed? | 213 |
| I. The Growth of $\pi(x)$ | 214 |
| A. History Unfolding | 215 |
| B. Sums Involving the Möbius Function | 229 |
| C. Tables of Primes | 233 |
| D. The Exact Value of $\pi(x)$ and Comparison with $x/(\log x)$, $\text{Li}(x)$, and $R(x)$ | 235 |
| E. The Nontrivial Zeros of $\zeta(s)$ | 239 |
| F. Zero-Free Regions for $\zeta(s)$ and the Error Term in the Prime Number Theorem | 243 |

| | |
|---|-----|
| G. The Growth of $\zeta(s)$ | 245 |
| H. Some Properties of $\pi(x)$ | 247 |
| II. The n th Prime and Gaps | 248 |
| A. The n th Prime | 248 |
| B. Gaps Between Primes | 250 |
| Interlude | 258 |
| III. Twin Primes | 259 |
| Addendum on k -Tuples of Primes | 265 |
| IV. Primes in Arithmetic Progression | 265 |
| A. There Are Infinitely Many! | 265 |
| B. The Smallest Prime in an Arithmetic Progression | 277 |
| C. Strings of Primes in Arithmetic Progression | 284 |
| V. Primes in Special Sequences | 288 |
| VI. Goldbach's Famous Conjecture | 291 |
| VII. The Waring–Goldbach Problem | 299 |
| A. Waring's Problem | 300 |
| B. The Waring–Goldbach Problem | 310 |
| VIII. The Distribution of Pseudoprimes, Carmichael Numbers, and Values of Euler's Function | 311 |
| A. Distribution of Pseudoprimes | 311 |
| B. Distribution of Carmichael Numbers | 314 |
| C. Distribution of Lucas Pseudoprimes | 317 |
| D. Distribution of Elliptic Pseudoprimes | 318 |
| E. Distribution of Values of Euler's Function | 319 |
| CHAPTER 5 | |
| Which Special Kinds of Primes Have Been Considered? | 323 |
| I. Regular Primes | 323 |
| II. Sophie Germain Primes | 329 |
| III. Wieferich Primes | 333 |
| IV. Wilson Primes | 346 |
| V. Repunits and Similar Numbers | 350 |
| VI. Primes with Given Initial and Final Digits | 355 |
| VII. Numbers $k \times 2^n \pm 1$ | 355 |
| VIII. Primes and Second-Order Linear Recurrence Sequences | 361 |
| IX. The NSW Primes | 367 |
| CHAPTER 6 | |
| Heuristic and Probabilistic Results about Prime Numbers | 371 |
| I. Prime Values of Linear Polynomials | 372 |
| II. Prime Values of Polynomials of Arbitrary Degree | 386 |
| III. Polynomials with Many Successive Composite Values | 400 |
| IV. Partitio Numerorum | 403 |
| V. Some Probabilistic Estimates | 411 |
| A. Distribution of Mersenne Primes | 411 |
| B. The log log Philosophy | 413 |
| VI. The Density of the Set of Regular Primes | 414 |

| | |
|------------------------------|-----|
| Conclusion | 427 |
| Bibliography | 433 |
| The Pages That Couldn't Wait | 509 |
| Primes up to 10,000 | 513 |
| Index of Tables | 517 |
| Index of Names | 519 |
| Subject Index | 535 |

Guiding the Reader

If a notation, which is not self-explanatory, appears without explanation on, say, page *xxx*, look at the Index of Notations, which is organized by page number; the definition of the notation should appear before page *xxx*.

If you wish to see where and how often your name is quoted in this book, turn to the Index of Names, at the end of the book. Should I say that there is no direct relation between achievement and number of quotes earned?

If, finally, you do not want to read the book but you just want to have some information about Knödel numbers—which is perfectly legitimate, if not laudable—go quickly to the Subject Index. Do not look under the heading “Numbers,” but rather “Knödel.” For a subject like “Strong Lucas pseudo-primes,” you have exactly three possibilities

Index of Notations

The following traditional notations are used in the text without explanation:

| Notation | Explanation |
|--------------------|---|
| $m n$ | the integer m divides the integer n |
| $m \nmid n$ | the integer m does not divide the integer n |
| $p^e \parallel n$ | p is a prime, $p^e n$ but $p^{e+1} \nmid n$ |
| $\gcd(m, n)$ | greatest common divisor of the integers m, n |
| $\text{lcm}(m, n)$ | least common multiple of the integers m, n |
| $\log x$ | natural logarithm of the real number $x > 0$ |
| \mathbb{Z} | ring of integers |
| \mathbb{Q} | field of rational numbers |
| \mathbb{R} | field of real numbers |
| \mathbb{C} | field of complex numbers |

The following notations are listed in the order that they appear in the book:

| Page | Notation | Explanation |
|------|----------|---|
| 3 | p_n | the n th prime |
| 4 | F_n | n th Fermat number, $F_n = 2^{2^n} + 1$ |
| 12 | $p^\#$ | product of all primes q , $q \leq p$ |
| 24 | g_p | smallest primitive root modulo p |
| 29 | $[x]$ | the largest integer in x , that is, the only integer such that $[x] \leq x < [x] + 1$ |

| Page | Notation | Explanation |
|------|--|---|
| 34 | $\varphi(n)$ | totient or Euler's function |
| 35 | $\lambda(n)$ | Carmichael's function |
| 37 | $\omega(n)$ | number of distinct prime factors of n |
| 37 | $L(x)$ | number of composite n , such that $n \leq x$ and $\varphi(n)$ divides $n - 1$ |
| 38 | $V_\varphi(m)$ | $\#\{n \geq 1 \mid \varphi(n) = m\}$ |
| 39 | $V_\varphi(m)$ | $= \#\{n \geq 1 \mid \varphi(n) = m\}$, valence function of φ |
| 42 | $E_\varphi(k)$ | $\#\{(n, m) \mid n > m \geq 1, n - m = k,$ $\varphi(n) = \varphi(m)\}$ |
| 44 | t_n^* | primitive part of $a^n - b^n$ |
| 44 | $k(m)$ | square-free kernel of m |
| 45 | $P[m]$ | largest prime factor of m |
| 45 | S_κ | set of integers n with at most $\{\kappa \log \log n\}$ distinct prime factors |
| 46 | (a/p) | Legendre symbol |
| 47 | (a/b) | Jacobi symbol |
| 55 | $U_n = U_n(P, Q)$ | n th term of the Lucas sequence with parameters (P, Q) |
| 55 | $V_n = V_n(P, Q)$ | n th term of the companion Lucas sequence with parameters (P, Q) |
| 60 | $\rho_u(n) = \rho(n, U)$ | smallest $r \geq 1$ such that $\rho(n)$ divides U_r |
| 61 | $\psi(p)$ | $p - (D/p)$ |
| 62 | $\left(\frac{\alpha, \beta}{p}\right)$ | a symbol associated to the roots α, β of $X^2 - PX + Q$ |
| 63 | $\lambda_{\alpha, \beta}(\prod p^e)$ | $\text{lcm}\{\psi_{\alpha, \beta}(p^e)\}$ |
| 66 | $\mathcal{P}(U)$ | set of primes p dividing some term U_n |
| 66 | $\mathcal{P}(V)$ | set of primes p dividing some term V_n |
| 69 | U_n^* | primitive part of U_n |
| 74 | $U_n = U_n(\sqrt{R}, Q)$ | n th term of the Lehmer sequence with parameters \sqrt{R}, Q |
| 74 | $V_n = V_n(\sqrt{R}, Q)$ | n th term of the companion Lehmer sequences with parameters \sqrt{R}, Q |
| 75 | $\psi_D\left(\prod_{i=1}^s p_i^{e_i}\right)$ | $= \frac{1}{2^{s-1}} \prod_{i=1}^s p_i^{e_i-1} \left(p_i - \left(\frac{D}{p_i}\right)\right)$ |

| Page | Notation | Explanation |
|------|-------------------------|---|
| 90 | M_q | Mersenne number, $M_q = 2^q - 1$ |
| 101 | $\tau(N)$ | number of divisors of N |
| 101 | $H(N)$ | harmonic mean of divisors of N |
| 102 | $V(x)$ | $\#\{N \text{ perfect number} \mid N \leq x\}$ |
| 103 | $s(N)$ | sum of aliquot parts of N |
| 103 | $\sigma(N)$ | sum of divisors of N |
| 105 | psp | pseudoprime in base 2 |
| 108 | $\text{psp}(a)$ | pseudoprime in base a |
| 110 | $B_{\text{psp}}(n)$ | number of bases a , $1 < a \leq n - 1$, $\gcd(a, n) = 1$, such that n is $\text{psp}(a)$ $e^{\log x \log \log \log x / \log \log x}$ |
| 111 | $l(x)$ | |
| 112 | $\text{epsp}(a)$ | Euler pseudoprime in base a |
| 113 | $B_{\text{epsp}}(n)$ | number of bases a , $1 < a \leq n - 1$, $\gcd(a, n) = 1$, such that n is $\text{epsp}(a)$ |
| 113 | $\text{spsp}(a)$ | strong pseudoprime in base a |
| 115 | $B_{\text{spsp}}(n)$ | number of bases a , $1 < a \leq n - 1$, $\gcd(a, n) = 1$, such that n is $\text{spsp}(a)$ |
| 117 | $R_{(a,b,k)}$ | set of all composite integers $n > k$ such that $a^{n-k} \equiv b^{n-k} \pmod{n}$ |
| 120 | $M_3(m)$ | $(6m + 1)(12m + 1)(18m + 1)$ |
| 120 | $M_k(m)$ | $(6m + 1)(12m + 1) \sum_{i=1}^{k-2} (9 \times 2^i m + 1)$ |
| 125 | C_k | set of all composite integers $n > k$ such that if $1 < a < n$, $\gcd(a, n) = 1$, then $a^{n-k} \equiv 1 \pmod{n}$ (the Knödel numbers when $k > 1$) |
| 127 | $\text{lpsp}(P, Q)$ | Lucas pseudoprime with parameters (P, Q) |
| 129 | $B_{\text{lpsp}}(n, Q)$ | number of integers P , $1 \leq P \leq n$, such that there exists Q , with $P^2 - 4Q \equiv D \pmod{n}$ and n is a $\text{lpsp}(P, Q)$ |
| 130 | $\text{elpsp}(P, Q)$ | Euler–Lucas pseudoprime with parameters (P, Q) |
| 130 | $\text{slpsp}(P, Q)$ | strong Lucas pseudoprime with parameters (P, Q) |
| 142 | $\pi(x)$ | the number of primes p , $p \leq x$ |
| 183 | $\mu(n)$ | Möbius function |

| Page | Notation | Explanation |
|------|-------------------------|---|
| 197 | $\pi_{f(x)}(x)$ | $\#\{n 1 \leq n \leq x, f(n) \text{ is a prime}\}$ |
| 203 | $v(f, N)$ | $\#\{x x = 0, 1, \dots, N \text{ such that } f(x) \text{ is equal to 1 or to a prime}\}$ |
| 205 | $P_0[m]$ | smallest prime factor of $m > 1$ |
| 206 | $h(d)$ | class number of $Q(\sqrt{d})$ |
| 214 | $f(x) \sim h(x)$ | f, h are asymptotically equal |
| 214 | $f(x) = g(x) + O(h(x))$ | the difference $f(x) - g(x)$ is ultimately bounded by a constant multiple of $h(x)$ |
| 215 | $f(x) = g(x) + o(h(x))$ | the difference $f(x) - g(x)$ is negligible in comparison to $h(x)$ |
| 216 | $\zeta(s)$ | Riemann's zeta function |
| 218 | B_k | Bernoulli number |
| 218 | $S_k(n)$ | $= \sum_{j=1}^n j^k$ |
| 219 | $B_k(X)$ | Bernoulli polynomial |
| 220 | $\text{Li}(x)$ | logarithmic integral |
| 221 | $\theta(x)$ | $= \sum_{p \leq x} \log p$, Tschebycheff function |
| 222 | $\text{Re}(s)$ | real part of s |
| 222 | $\Gamma(s)$ | gamma function |
| 224 | $J(x)$ | weighted prime-power counting function |
| 224 | $R(x)$ | Riemann's function |
| 226 | $\Lambda(n)$ | von Mangoldt's function |
| 227 | γ | Euler's constant |
| 227 | $\psi(x)$ | summatory function of the von Mangoldt function |
| 230 | $f * g$ | convolution of arithmetic functions |
| 230 | $M(x)$ | Mertens's function |
| 236 | $\varphi(x, m)$ | $= \#\{a 1 \leq a \leq x, a \text{ is not a multiple of } 2, 3, \dots, p_m\}$ |
| 240 | $N(T)$ | $= \#\{\rho = \sigma + it 0 \leq \sigma \leq 1, \zeta(\rho) = 0, 0 < t \leq T\}$ |
| 240 | ρ_n | n th zero of $\zeta(s)$ in the upper half of the critical strip |
| 240 | $N(\sigma, t)$ | number of zeros $\rho = \beta + it$ of $\zeta(s)$, with $\sigma \leq \beta$ and $0 < t \leq T$ |

| Page | Notation | Explanation |
|------|------------------------|---|
| 245 | $\omega(\sigma)$ | $= \inf\{\alpha > 0 \mid \zeta(\sigma + it) = O(t^\alpha)\}$ |
| 250 | d_n | $= p_{n+1} - p_n$ |
| 250 | $g(p)$ | number of successive composite integers greater than p |
| 255 | $\log_2 x$ | $\log \log x$ |
| 255 | $\log_3 x$ | $\log \log \log x$ |
| 255 | $\log_4 x$ | $\log \log \log \log x$ |
| 258 | $\pi_{f(x)}(x)$ | $\#\{n \geq 1 \mid f(n) \leq x, f(n) \in P_k\}$ |
| 259 | P_k | set of all k -almost-primes |
| 259 | $\pi_{f(x)}^{(k)}(x)$ | $= \{n \leq x \mid f(n) \in P_k\}$ |
| 259 | $\pi_{f(x)}^{(k)*}(x)$ | $= \{n \geq 1 \mid f(n) \in P_k, f(n) \leq x\}$ |
| 259 | $\pi_{f(x)}^{(k)}(x)$ | $= \#\{n \geq 1 \mid f(n) \leq x \text{ and } f(n) \in P_k\}$ |
| 260 | $\pi_2(x)$ | $= \#\{p \text{ prime} \mid p \leq x \text{ and } p+2 \text{ is also a prime}\}$ |
| 261 | B | Brun's constant |
| 262 | C_2 | $= \prod_{p>2} (1 - 1/(p-1)^2)$, twin prime constant |
| 264 | $\pi_{2k}(x)$ | $= \#\{n \geq 1 \mid p_n \leq x \text{ and } p_{n+1} - p_n = 2k\}$ |
| 266 | ζ_n | $= \cos 2\pi/n + i \sin 2\pi/n$ |
| 266 | $\Phi_n(X)$ | n th cyclotomic polynomial |
| 271 | $\mathcal{P}(f)$ | set of all primes p dividing $f(n)$, for some integer n |
| 273 | χ | modular character |
| 273 | $L(s \chi)$ | L -function associated to the character χ |
| 274 | $\pi_{d,a}(x)$ | $= \#\{p \text{ prime} \mid p \leq x, p \equiv a \pmod{d}\}$ |
| 277 | $p(d, a)$ | smallest prime in the arithmetic progression $\{a + kd \mid k \geq 0\}$ |
| 277 | $p(d)$ | $= \max\{p(d, a) \mid 1 \leq a < d, \gcd(a, d) = 1\}$ |
| 279 | L | Linnik's constant |
| 280 | $g(m)$ | Jacobsthal function |
| 283 | $P_k(d, a)$ | smallest k -almost-prime in the arithmetic progression $\{a + nd \mid n \geq 1\}$ |

| Page | Notation | Explanation |
|------|------------------|--|
| 285 | $N_m(x)$ | $= \# \{ \text{arithmetic progressions of primes } p_1 < p_2 < \cdots < p_m \leq x \}$ |
| 289 | $I(A, n)$ | $= \# \{ i 1 \leq i \leq n, \alpha_i \in I \}$ |
| 289 | $\pi_\alpha(x)$ | $= \# \{ p \text{ prime} p \leq x \text{ and there exists } k \geq 1 \text{ such that } p = [k\alpha] \}$ |
| 290 | $\pi^\alpha(x)$ | $= \# \{ p \text{ prime} p \leq x \text{ and there exists } k \geq 1 \text{ such that } p = [k^\alpha] \}$ |
| 293 | $d(A)$ | density of the sequence A |
| 293 | S, S_0 | Schnirelman's constants |
| 297 | $r_2(2n)$ | number of representations of $2n$ as sums of two primes |
| 297 | $r_3(n)$ | number of representations of the odd number n as sums of three primes |
| 298 | $G'(x)$ | $= \# \{ 2n 2n \leq x, 2n \text{ is not a sum of two primes} \}$ |
| 300 | $g(k)$ | smallest integer r such that every natural number is the sum of at most r k th powers |
| 300 | $G(k)$ | smallest integer r such that every sufficiently large integer is the sum of at most r k th powers |
| 309 | $V(k)$ | smallest integer r such that every sufficiently large integer is the sum of at most r k th powers of prime numbers |
| 310 | $(\text{psp})_n$ | n th pseudoprime |
| 310 | $P\pi(x)$ | number of pseudoprimes to base 2, less than or equal to x |
| 311 | $P\pi_a(x)$ | number of pseudoprimes to base a , less than or equal to x |
| 311 | $EP\pi(x)$ | number of Euler pseudoprimes to base 2, less than or equal to x |
| 311 | $EP\pi_a(x)$ | same, to base a |
| 311 | $SP\pi(x)$ | number of strong pseudoprimes to base 2, less than or equal to x |
| 311 | $SP\pi_a(x)$ | same, to base a |

| Page | Notation | Explanation |
|------|-----------------------|---|
| 313 | $\text{psp}(d, a)$ | smallest pseudoprime in the arithmetic progression $\{a + kd \mid k \geq 1\}$ with $\gcd(a, d) = 1$ |
| 314 | $CN(x)$ | $= \#\{n \mid n \leq x, n \text{ Carmichael number}\}$ |
| 317 | $L\pi(x)$ | number of Lucas pseudoprimes [with parameters (P, Q)] $n \leq x$ |
| 317 | $SL\pi(x)$ | number of strong Lucas pseudoprimes [with parameters (P, Q)] $n \leq x$ |
| 321 | $V_\phi^\#(m)$ | $= \#\{k \mid 1 \leq k \leq m, \text{ there exists } n \geq 1 \text{ with } \phi(n) = k\}$ |
| 325 | $\pi_{\text{reg}}(N)$ | number of regular primes $p \leq x$ |
| 325 | $\pi_{\text{ir}}(x)$ | number of irregular primes $p \leq x$ |
| 326 | $\text{ii}(p)$ | irregularity index of p |
| 326 | $\pi_{\text{iis}}(x)$ | number of primes $p \leq x$ such that $\text{ii}(p) = s$ |
| 327 | K_n | $= \mathbb{Q}(\zeta_{p^{n+1}})$ |
| 327 | K_n^+ | $= \mathbb{Q}(\zeta_{p^{n+1}} + \zeta_{p^{n+1}}^{-1})$ |
| 327 | h_n | class number of K_n |
| 327 | h_n^+ | class number of K_n^+ |
| 331 | $S_{d,a}(x)$ | $= \#\{p \text{ prime} \mid p \leq x, a + pd \text{ is a prime}\}$ |
| 335 | $q_p(a)$ | $= (a^{p-1} - 1)/p$, Fermat quotient of p , with base a |
| 336 | $\mathcal{W}_l^{(k)}$ | $= \{p \text{ prime} \mid l^{p-1} \equiv 1 \pmod{p^k}\}$ |
| 337 | \mathcal{N}_L | $= \{p \text{ prime} \mid \text{there exists } c, \text{ not a multiple of } p, \text{ such that } pc = u \pm v, \text{ where all prime factors of } uv \text{ are at most } L\}$ |
| 338 | $\mathcal{N}_l^{(k)}$ | $= \{p \text{ prime} \mid \text{there exists } s \geq 1 \text{ such that } p \text{ divides } l^s + 1, \text{ but } p^{k+1} \text{ does not divide } l^s + 1\}$ |
| 344 | $\mathcal{P}(F)$ | $= \{p \text{ prime} \mid \text{there exists } n \text{ such that } p \text{ divides } F_n\}$ |
| 344 | $\mathcal{P}(M)$ | $= \{p \text{ prime} \mid \text{there exists a prime } q \text{ such that } p \text{ divides } M_q\}$ |

| Page | Notation | Explanation |
|------|------------------------------------|--|
| 344 | $\mathcal{P}^{(2)}(F)$ | $= \{p \text{ prime} \text{there exists } n \text{ such that } p^2 \text{ divides } F_n\}$ |
| 344 | $\mathcal{P}^{(2)}(M)$ | $= \{p \text{ prime} \text{there exists a prime } q \text{ such that } p^2 \text{ divides } M_q\}$ |
| 350 | R_n | $= (10^n - 1)/9$, repunit |
| 350 | P_n | prime with n digits |
| 356 | $N(x)$ | $=$ number of odd integers k , $1 \leq k \leq x$, such that there exists $n \geq 1$ for which $k \times 2^n + 1$ is a prime |
| 360 | C_n | $n \times 2^n + 1$, Cullen number |
| 361 | $C\pi(x)$ | number of Cullen numbers $Cn \leq x$ that are prime |
| 365 | $\mathcal{P}(T)$ | set of primes p dividing some term of the sequence $T = (T_n)_{n \geq 0}$ |
| 367 | S_{2m+1} | NSW-number |
| 368 | \mathbf{F}_P | field with P elements |
| 368 | $\text{Sp}(2n, \mathbf{F}_P)$ | symplectic group of dimension $2n$ over \mathbf{F}_P |
| 383 | $\text{prim}_g(x)$ | $= \#\{p \text{ prime} p \leq x, g \text{ is a primitive root modulo } p\}$ |
| 384 | A | $= \prod_{p \geq 2} (1 - 1/p(p-1))$, Artin's constant |
| 396 | $\rho(x)$ | $\limsup_{y \rightarrow \infty} (\pi(y+x) - \pi(y))$ |
| 400 | $p(f)$ | smallest integer $m \geq 1$ such that $ f(m) $ is a prime |
| 403 | $k(d, u)$ | smallest integer $k \geq 1$ such that $X^d + k$ is irreducible, satisfies condition $(*)$ and $p(X^d + k) > u$ |
| 405 | $\pi_{X^2+1}^*(x)$ | $= \#\{p \text{ prime} p \text{ is of the form } p = m^2 + 1, \text{ and } p \leq x\}$ |
| 406 | $\pi_{aX^2+bX+c}^*(x)$ | $= \#\{p \text{ prime} p \text{ is of the form } p = am^2 + bm + c, \text{ and } p \leq x\}$ |
| 407 | $\pi_{X^3+k}^*(x)$ | $= \#\{p \text{ prime} p \text{ is of the form } p = m^3 + k, \text{ and } p \leq x\}$ |
| 408 | $\pi_{X^3+Y^3+Z^3}^*(x)$ | $= \#\{(k, l, m) 1 \leq k, l, m, \text{ and } k^3 + l^3 + m^3 = p \leq x, p \text{ prime}\}$ |
| 410 | $\mathcal{Q}_{f_1, \dots, f_s}(N)$ | $= \#\{n 1 \leq n \leq N, f_1(n), \dots, f_s(n) \text{ are primes}\}$ |