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.

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 $\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$.

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 trible 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

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 pseudoprimes," you have exactly three possibilities ....

Index of Notations

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

Notation	Explanation
$m \mid n$	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, $p^e \mid n$ but $p^{e+1} \nmid n$
$\gcd(m, n)$	greatest common divisor of the integers m, n
$\operatorname{lcm}(m, n)$	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 nth prime
4	F_n	nth 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	$U_n = U_n(P, Q)$	nth term of the Lucas sequence with parameters (P, Q)
55	$V_n = V_n(P, Q)$	nth 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	$\left(\dfrac{\alpha, \beta}{p}\right)$	a symbol associated to the roots α, β of $X^2 - PX + Q$
63	$\lambda_{\alpha,\beta}(\prod p^e)$	$\operatorname{lcm}\{\psi_{\alpha,\beta}(p^e)\}$
66	$\mathscr{P}(U)$	set of primes p dividing some term U_n
66	$\mathscr{P}(V)$	set of primes p dividing some term V_n
69	U_n^*	primitive part of U_n
74	$U_n = U_n(\sqrt{R}, Q)$	nth term of the Lehmer sequence with parameters $\sqrt{R}, Q$
74	$V_n = V_n(\sqrt{R}, Q)$	nth term of the companion Lehmer sequences with parameters $\sqrt{R}, Q$
75	$\psi_D\left(\prod_{i=1}^{s} p_i^{e_i}\right)$	$= \dfrac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1}\left(p_i - \left(\dfrac{D}{p_i}\right)\right)$

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	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 psp(a)
111	$l(x)$	$e^{\log x \log\log\log x/\log\log x}$
112	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 epsp(a)
113	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 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	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 lpsp(P, Q)
130	elpsp(P, Q)	Euler–Lucas pseudoprime with parameters (P, Q)
130	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
245	$\omega(\sigma)$	$= \inf\{\alpha > 0 \mid \lvert\zeta(\sigma + it)\rvert = O(t^\alpha)\}$
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	$\pi_{f(X)}(x)$	$\#\{n \geq 1 \mid \lvert f(n)\rvert \leq x, \lvert f(n)\rvert \in P_k\}$
259	P_k	set of all k-almost-primes
259	$\pi^{(k)}_{f(X)}(x)$	$= \{n \leq x \mid \lvert f(n)\rvert \in P_k\}$
259	$\pi^{(k)*}_{f(X)}(x)$	$= \{n \geq 1 \mid \lvert f(n)\rvert \in P_k, \lvert f(n)\rvert \leq x\}$
259	$\pi^{(k)}_{f(X)}(x)$	$= \#\{n \geq 1 \mid \lvert f(n)\rvert \leq x$ and $\lvert f(n)\rvert \in P_k\}$
260	$\pi_2(x)$	$= \#\{p$ prime $\mid p \leq x$ and $p + 2$ is also a prime$\}$
261	B	Brun's constant
262	C_2	$= \prod_{p>2}(1 - 1/(p-1)^2)$, twin prime constant
264	$\pi_{2k}(x)$	$= \#\{n \geq 1 \mid p_n \leq x$ and $p_{n+1} - p_n = 2k\}$
266	ζ_n	$= \cos 2\pi/n + i \sin 2\pi/n$
266	$\Phi_n(X)$	nth cyclotomic polynomial
271	$\mathscr{P}(f)$	set of all primes p dividing $f(n)$, for some integer n
273	χ	modular character
273	$L(s \mid \chi)$	L-function associated to the character χ
274	$\pi_{d,a}(x)$	$= \#\{p$ 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	$N_m(x)$	$= \#\{$arithmetic progressions of primes $p_1 < p_2 < \cdots < p_m \leq x\}$
289	$I(A, n)$	$= \#\{i \mid 1 \leq i \leq n, \alpha_i \in I\}$
289	$\pi_\alpha(x)$	$= \#\{p$ prime$\mid p \leq x$ and there exists $k \geq 1$ such that $p = [k\alpha]\}$
290	$\pi^\alpha(x)$	$= \#\{p$ prime$\mid p \leq x$ and there exists $k \geq 1$ 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	$G'(x)$	$= \#\{2n \mid 2n \leq x, 2n$ 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 kth powers
300	$G(k)$	smallest integer r such that every sufficiently large integer is the sum of at most r kth powers
309	$V(k)$	smallest integer r such that every sufficiently large integer is the sum of at most r kth powers of prime numbers
310	$(\mathrm{psp})_n$	nth 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	$\mathrm{psp}(d, a)$	smallest pseudoprime in the arithmetic progression $\{a + kd \mid k \geq 1\}$ with $\gcd(a, d) = 1$
314	$CN(x)$	$= \#\{n \mid n \leq x, n$ 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	$V_\varphi^\#(m)$	$= \#\{k \mid 1 \leq k \leq m$, there exists $n \geq 1$ with $\varphi(n) = k\}$
325	$\pi_{\mathrm{reg}}(N)$	number of regular primes $p \leq x$
325	$\pi_{\mathrm{ir}}(x)$	number of irregular primes $p \leq x$
326	$\mathrm{ii}(p)$	irregularity index of p
326	$\pi_{\mathrm{iis}}(x)$	number of primes $p \leq x$ such that $\mathrm{ii}(p) = s$
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	$S_{d,a}(x)$	$= \#\{p$ prime$\mid p \leq x$, $a + pd$ is a prime$\}$
335	$q_p(a)$	$= (a^{p-1} - 1)/p$, Fermat quotient of p, with base a
336	$\mathscr{W}_l^{(k)}$	$= \{p$ prime$\mid l^{p-1} \equiv 1 \pmod{p^k}\}$
337	$\mathscr{N}_L$	$= \{p$ prime$\mid$there exists c, not a multiple of p, such that $pc = u \pm v$, where all prime factors of uv are at most $L\}$
338	$\mathscr{N}_l^{(k)}$	$= \{p$ prime$\mid$there exists $s \geq 1$ such that p divides $l^s + 1$, but p^{k+1} does not divide $l^s + 1\}$
344	$\mathscr{P}(F)$	$= \{p$ prime$\mid$there exists n such that p divides $F_n\}$
344	$\mathscr{P}(M)$	$= \{p$ prime$\mid$there exists a prime q such that p divides $M_q\}$

Page	Notation	Explanation
344	$\mathscr{P}^{(2)}(F)$	$= \{p$ prime$\mid$there exists n such that p^2 divides $F_n\}$
344	$\mathscr{P}^{(2)}(M)$	$= \{p$ prime$\mid$there exists a prime q such that p^2 divides $M_q\}$
350	Rn	$= (10^n - 1)/9$, repunit
350	Pn	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	$\mathscr{P}(T)$	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	$\mathrm{Sp}(2n, \mathbf{F}_P)$	symplectic group of dimension $2n$ over $\mathbf{F}_P$
383	$\mathrm{prim}_g(x)$	$= \#\{p$ prime$\mid p \leq x$, g is a primitive root modulo $p\}$
384	A	$= \prod_{p \geq 2}(1 - 1/p(p-1))$, Artin's constant
396	$\rho(x)$	$\limsup_{y \to \infty} (\pi(y + x) - \pi(y))$
400	$p(f)$	smallest integer $m \geq 1$ such that $\lvert f(m)\rvert$ 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	$\pi^*_{X^2+1}(x)$	$= \#\{p$ prime$\mid p$ is of the form $p = m^2 + 1$, and $p \leq x\}$
406	$\pi^*_{aX^2+bX+c}(x)$	$= \#\{p$ prime$\mid p$ is of the form $p = am^2 + bm + c$, and $p \leq x\}$
407	$\pi^*_{X^3+k}(x)$	$= \#\{p$ prime$\mid p$ is of the form $p = m^3 + k$, and $p \leq x\}$
408	$\pi^*_{X^3+Y^3+Z^3}(x)$	$= \#\{(k, l, m)\mid 1 \leq k, l, m$, and $k^3 + l^3 + m^3 = p \leq x$, p prime$\}$
410	$Q_{f_1,\ldots,f_s}(N)$	$= \#\{n\mid 1 \leq n \leq N$, $f_1(n), \ldots, f_s(n)$ are primes$\}$