Not Always Buried Deep

A Second Course in Elementary Number Theory

Paul Pollack

American Mathematical Society
Not Always Buried Deep
A Second Course in Elementary Number Theory
Not Always Buried Deep
A Second Course in Elementary Number Theory

Paul Pollack
Dedicated to the memory of Arnold Ephraim Ross (1906–2002)
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>xi</td>
</tr>
<tr>
<td>Notation</td>
<td>xiii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>xiv</td>
</tr>
<tr>
<td>Chapter 1. Elementary Prime Number Theory, I</td>
<td>1</td>
</tr>
<tr>
<td>§1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>§2. Euclid and his imitators</td>
<td>2</td>
</tr>
<tr>
<td>§3. Coprime integer sequences</td>
<td>3</td>
</tr>
<tr>
<td>§4. The Euler-Riemann zeta function</td>
<td>4</td>
</tr>
<tr>
<td>§5. Squarefree and smooth numbers</td>
<td>9</td>
</tr>
<tr>
<td>§6. Sledgehammers!</td>
<td>12</td>
</tr>
<tr>
<td>§7. Prime-producing formulas</td>
<td>13</td>
</tr>
<tr>
<td>§8. Euler’s prime-producing polynomial</td>
<td>14</td>
</tr>
<tr>
<td>§9. Primes represented by general polynomials</td>
<td>22</td>
</tr>
<tr>
<td>§10. Primes and composites in other sequences</td>
<td>29</td>
</tr>
<tr>
<td>Notes</td>
<td>32</td>
</tr>
<tr>
<td>Exercises</td>
<td>34</td>
</tr>
<tr>
<td>Chapter 2. Cyclotomy</td>
<td>45</td>
</tr>
<tr>
<td>§1. Introduction</td>
<td>45</td>
</tr>
<tr>
<td>§2. An algebraic criterion for constructibility</td>
<td>50</td>
</tr>
<tr>
<td>§3. Much ado about $\mathbb{Z}[\zeta_p]$</td>
<td>52</td>
</tr>
<tr>
<td>§4. Completion of the proof of the Gauss–Wantzel theorem</td>
<td>55</td>
</tr>
<tr>
<td>§5. Period polynomials and Kummer’s criterion</td>
<td>57</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>3</td>
<td>Elementary Prime Number Theory, II</td>
</tr>
<tr>
<td>2</td>
<td>The set of prime numbers has density zero</td>
</tr>
<tr>
<td>3</td>
<td>Three theorems of Chebyshev</td>
</tr>
<tr>
<td>4</td>
<td>The work of Mertens</td>
</tr>
<tr>
<td>5</td>
<td>Primes and probability</td>
</tr>
<tr>
<td>6</td>
<td>Introduction</td>
</tr>
<tr>
<td>4</td>
<td>Primes in Arithmetic Progressions</td>
</tr>
<tr>
<td>2</td>
<td>Progressions modulo 4</td>
</tr>
<tr>
<td>3</td>
<td>The characters of a finite abelian group</td>
</tr>
<tr>
<td>4</td>
<td>The $L$-series at $s = 1$</td>
</tr>
<tr>
<td>5</td>
<td>Nonvanishing of $L(1, \chi)$ for complex $\chi$</td>
</tr>
<tr>
<td>6</td>
<td>Nonvanishing of $L(1, \chi)$ for real $\chi$</td>
</tr>
<tr>
<td>7</td>
<td>Finishing up</td>
</tr>
<tr>
<td>8</td>
<td>Sums of three squares</td>
</tr>
<tr>
<td>5</td>
<td>Interlude: A Proof of the Hilbert–Waring Theorem</td>
</tr>
<tr>
<td>2</td>
<td>Proof of the Hilbert–Waring theorem (Theorem 5.1)</td>
</tr>
<tr>
<td>3</td>
<td>Producing the Hilbert–Dress identities</td>
</tr>
<tr>
<td>6</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>The general sieve problem: Notation and preliminaries</td>
</tr>
<tr>
<td>3</td>
<td>The sieve of Eratosthenes–Legendre and its applications</td>
</tr>
<tr>
<td>4</td>
<td>Brun’s pure sieve</td>
</tr>
<tr>
<td>5</td>
<td>The Brun–Hooley sieve</td>
</tr>
</tbody>
</table>
Foreword

The gold in ‘them there hills’ is not always buried deep. Much of it is within easy reach. Some of it is right on the surface to be picked up by any searcher with a keen eye for detail and an eagerness to explore. As in any treasure hunt, the involvement grows as the hunt proceeds and each success whether small or great adds the fuel of excitement to the exploration. – A. E. Ross

Number theory is one of the few areas of mathematics where problems of substantial interest can be described to someone possessing scant mathematical background. It sometimes proves to be the case that a problem which is simple to state requires for its resolution considerable mathematical preparation; e.g., this appears to be the case for Fermat’s conjecture regarding integer solutions to the equation $x^n + y^n = z^n$. But this is by no means a universal phenomenon; many engaging problems can be successfully attacked with little more than one’s “mathematical bare hands”. In this case one says that the problem can be solved in an elementary way (even though the elementary solution may be far from simple). Such elementary methods and the problems to which they apply are the subject of this book.

Because of the nature of the material, very little is required in terms of prerequisites: The reader is expected to have prior familiarity with number theory at the level of an undergraduate course. The necessary background can be gleaned from any number of excellent texts, such as Sierpiński’s charmingly discursive Elementary Theory of Numbers or LeVeque’s lucid and methodical Fundamentals of Number Theory. Apart from this, a rigorous course in calculus, some facility with manipulation of estimates (in
particular, big-Oh and little-oh notation), and a first course in modern algebra (covering groups, rings, and fields) should suffice for the majority of the text. A course in complex variables is not required, provided that the reader is willing to overlook some motivational remarks made in Chapter 7.

Rather than attempt a comprehensive account of elementary methods in number theory, I have focused on topics that I find particularly attractive and accessible:

- Chapters 1, 3, 4, and 7 collectively provide an overview of prime number theory, starting from the infinitude of the primes, moving through the elementary estimates of Chebyshev and Mertens, then the theorem of Dirichlet on primes in prescribed arithmetic progressions, and culminating in an elementary proof of the prime number theorem.

- Chapter 2 contains a discussion of Gauss’s arithmetic theory of the roots of unity (cyclotomy), which was first presented in the final section of his Disquisitiones Arithmeticae. After developing this theory to the extent required to prove Gauss’s characterization of constructible regular polygons, we give a cyclotomic proof of the quadratic reciprocity law, followed by a detailed account of a little-known cubic reciprocity law due to Jacobi.

- Chapter 5 is a 12-page interlude containing Dress’s proof of the following result conjectured by Waring in 1770 and established by Hilbert in 1909: For each fixed integer \( k \geq 2 \), every natural number can be expressed as the sum of a bounded number of nonnegative \( k \)th powers, where the bound depends only on \( k \).

- Chapter 6 is an introduction to combinatorial sieve methods, which were introduced by Brun in the early twentieth century. The best-known consequence of Brun’s method is that if one sums the reciprocals of each prime appearing in a twin prime pair \( p, p+2 \), then the answer is finite. Our treatment of sieve methods is robust enough to establish not only this and other comparable ‘upper bound’ results, but also Brun’s deeper “lower bound” results. For example, we prove that there are infinitely many \( n \) for which both \( n \) and \( n+2 \) have at most 7 prime factors, counted with multiplicity.

- Chapter 8 summarizes what is known at present about perfect numbers, numbers which are the sum of their proper divisors.

At the end of each chapter (excepting the interlude) I have included several nonroutine exercises. Many are based on articles from the mathematical literature, including both research journals and expository publications like the American Mathematical Monthly. Here, as throughout the text, I have
made a conscious effort to document original sources and thus encourage conformance to Abel’s advice to “read the masters”.

While the study of elementary methods in number theory is one of the most accessible branches of mathematics, the lack of suitable textbooks has been a repellent to potential students. It is hoped that this modest contribution will help to reverse this injustice.

Paul Pollack

Notation

While most of our notation is standard and should be familiar from an introductory course in number theory, a few of our conventions deserve explicit mention: The set $\mathbb{N}$ of natural numbers is the set $\{1, 2, 3, 4, \ldots\}$. Thus 0 is not considered a natural number. Also, if $n \in \mathbb{N}$, we write “$\tau(n)$” (instead of “$d(n)$”) for the number of divisors of $n$. This is simply to avoid awkward expressions like “$d(d)$” for the number of divisors of the natural number $d$. Throughout the book, we reserve the letter $p$ for a prime variable.

We remind the reader that “$A = O(B)$” indicates that $|A| \leq c|B|$ for some constant $c > 0$ (called the implied constant); an equivalent notation is “$A \ll B$”. The notation “$A \gg B$” means $B \ll A$, and we write “$A \asymp B$” if both $A \ll B$ and $A \gg B$. If $A$ and $B$ are functions of a single real variable $x$, we often speak of an estimate of this kind holding as “$x \to a$” (where $a$ belongs to the two-point compactification $\mathbb{R} \cup \{\pm \infty\}$ of $\mathbb{R}$) to mean that the estimate is valid on some deleted neighborhood of $a$. Subscripts on any of these symbols indicate parameters on which the implied constants (and, if applicable, the deleted neighborhoods) may depend. The notation “$A \sim B$” means $A/B \to 1$ while “$A = o(B)$” means $A/B \to 0$; here subscripts indicate parameters on which the rate of convergence may depend.

If $S$ is a subset of the natural numbers $\mathbb{N}$, the (asymptotic, or natural) density of $S$ is defined as the limit

$$\lim_{x \to \infty} \frac{1}{x} \#\{n \in S : n \leq x\},$$

provided that this limit exists. The lower density and upper density of $S$ are defined similarly, with $\liminf$ and $\limsup$ replacing $\lim$ (respectively). We say that a statement holds for almost all natural numbers $n$ if it holds on a subset of $\mathbb{N}$ of density 1.

If $f$ and $G$ are defined on a closed interval $[a, b] \subset \mathbb{R}$, with $f'$ piecewise continuous there, we define

$$(0.1) \quad \int_a^b f(t) \, dG(t) := G(b)f(b) - G(a)f(a) - \int_a^b f'(t)G(t) \, dt,$$
provided that the right-hand integral exists. (Experts will recognize the right-hand side as the formula for integration by parts for the Riemann–Stieltjes integral, but defining the left-hand side in this manner allows us to avoid assuming any knowledge of Riemann–Stieltjes integration.) We will often apply partial summation in the following form, which is straightforward to verify directly: Suppose that $a$ and $b$ are real numbers with $a \leq b$ and that we are given complex numbers $a_n$ for all natural numbers $n$ with $a < n \leq b$. Put $S(t) := \sum_{a < n \leq t} a_n$. If $f'$ is piecewise continuous on $[a, b]$, then

$$\sum_{a < n \leq b} a_n f(n) = \int_a^b f(t) \, dS(t).$$

In order to paint an accurate portrait of the mathematical landscape without straying off point, it has been necessary on occasion to state certain theorems without proof; such results are marked with a star ($\star$). For some of these results, proofs are sketched in the corresponding chapter exercises.

**Acknowledgements**

There are many people without whom this book could not have been written and many others without whom this book would not be worth reading.

Key members of the first group include my middle and high-school teachers Daniel Phelon, Sharon Bellak, and Jeff Miller. It is thanks to their tireless efforts that I was prepared to attend the Ross Summer Mathematics Program at Ohio State University in 1998. There Arnold Ross, assisted by my counselor Noah Snyder and my seminar instructor Daniel Shapiro, impressed upon me the importance of grappling with mathematical ideas for oneself. I regard this as the most important lesson I have learned so far on my mathematical journey. As an undergraduate, I was the fortunate recipient of generous mentoring from Andrew Granville and Matt Baker, and I had the privilege of attending A. J. Hildebrand’s 2002 REU in number theory. My subsequent graduate experience at Dartmouth College ranks as one of the happiest times of my life, due in large measure to the wise guidance of my advisor, Carl Pomerance.

My family — my father Lawrence, my mother Lolita, and my brother Michael — has done so much for me over the years that it would be impossible (and inappropriate!) for me to express the extent of my appreciation in this brief space. Another friend for whom I am grateful beyond words is Susan Roth, who for the last decade has accompanied me on many of my (mis)adventures in genre television.

Mits Kobayashi cheerfully donated his time to prepare many of the figures included in the text. Both he and Enrique Treviño pointed out several
typographical errors and inaccuracies in earlier versions of the manuscript. I am grateful for both their help and their friendship.

This text served as the basis for a graduate topics course taught by the author during the Spring 2009 semester at the University of Illinois at Urbana-Champaign. I am grateful to the U of I for allowing me this opportunity. Almost concurrently, Carl Pomerance used a preliminary version of these notes to teach a quarter-long course at Dartmouth College. This manuscript is better for his numerous insightful suggestions.

Finally, I would like to thank the American Mathematical Society, especially Ed Dunne, Cristin Zanella, and Luann Cole, for their encouragement of this project at every stage.
References


[And74] C. W. Anderson, The solutions of \( \Sigma(n) = \sigma(n) \), \( \Phi(n) = \varphi(n) \), and related considerations, unpublished manuscript, 1974.


[Ban91] A. S. Bang, Om Primtal af bestemte Former, Nyt Tidsskrift for matematik, B (advanced) 2 (1891), 73–82.


References


References

281


[Bru19a] _, La série $\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \frac{1}{41} + \frac{1}{43} + \frac{1}{59} + \frac{1}{61} + \cdots$ où les dénominateurs sont “nombres premiers jumeaux” est convergente ou finie, Bull. Sci. Math 43 (1919), 100–104, 124–128.


References


[Dic13b] ——, *Theorems and tables on the sum of the divisors of a number*, Quart. J. Math **44** (1913), 264–296.

References


[Dre71] F. Dress, Méthodes élémentaires dans le problème de Waring pour les entiers, Université de Provence, Marseille, 1971, Journées Arithmétiques Françaises, Mai 1971.


References


[Erd73], Über die Zahlen der Form \( \sigma(n) - n \) und \( n - \phi(n) \), Elem. Math. 28 (1973), 83–86.


<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
</table>
References


H. B. Mann, A proof of the fundamental theorem on the density of sums of sets of positive integers, Ann. of Math. (2) 43 (1942), 523–527.


References


[Pri01] W. Pribitkin, *Notes: A Simpler Proof of $\pi(z) = z \prod_{k=1}^{\infty} (1 - z^2/k^2)$*, Amer. Math. Monthly 108 (2001), no. 8, 767–768.


References


[Sch40] …, Prime numbers, State Publishing House of Technico-Theoretical Literature, Moscow, 1940.


[Sch62b] …, On the composite integers of the form $c(ak + b)! \pm 1$, Nordisk Mat. Tidskr. 10 (1962), 8–10.


[Sel49b] …, An elementary proof of the prime-number theorem, Ann. of Math. (2) 50 (1949), 305–313.


[SG] P. Sebah and X. Gourdon, Introduction to twin primes and Brun’s constant computation, available from the authors’ website at the URL http://numbers.computation.free.fr/Constants/constants.html.


[Sha64] D. Shanks, An analytic criterion for the existence of infinitely many primes of the form $\frac{1}{2}(n^2 + 1)$, Illinois J. Math. 8 (1964), 377–379.


References


References


References


Index

\( \Psi(x, y) \), 11, 115, 206
  upper bound for \( \Psi(x, \log x) \), 257
\( \gamma \), 98
Li(x), 86
\( \ll \) and \( \gg \), xiii
\( \omega(n) \) and \( \Omega(n) \), 111
\( \pi(x) \), 1
\( \sigma_{-1}(n) \), 254
\( \sim \), xiii
\( \zeta(s) \), 4
\( e^{\pi \sqrt{163}} \), 32
\( f \)-nomial period, see also Gaussian period
\( m \)-gonal number, 148
\( s(n) \), 248

abundant numbers, 248
density, 251
aliquot sequence, 252
geometric growth, 263, 268
almost prime, 168
amicable numbers, 252
Artin’s constant, 245

Bertrand’s postulate, 89, 94, 108
Besicovitch set, 276
big-Oh notation, xii, xiii
Bombieri–Vinogradov theorem, 109
Bonferroni inequalities, 177
Brun’s constant, 180
Brun’s method, 206
Brun’s pure sieve, 168, 175
  application to estimating \( \pi_2(x) \), 179
  general version, 178
  working version, 178
Brun–Hooley sieve, 168, 182
  application to sums of primes
    (Schnirelmann’s theorem), 196
  application to the generalized twin prime problem, 190, 196
  application to the Goldbach problem, 185, 193
  lower bound method, 191
  upper bound method, 183
Brun–Titchmarsh inequality, 206, 245, 273

Carathéodory’s theorem, 156
Cardano’s formula, 71
Catalan–Dickson conjecture, 253
character of a finite abelian group, 123
  characters of \( (\mathbb{Z}/m\mathbb{Z})^\times \), 124
  classification of characters, 124
  orthogonality relations, 125, 142
  trivial character, 123
Chebotarev density theorem, 26, 40
Chebyshev’s theorems, 89, 92, 217, 220
class number 1 problem, 22
class number 1 problem, 22
cluster prime, 204
composite numbers, 1
  of the form \( \alpha \cdot n! + 1 \), 31
  of the form \( \lfloor \xi \alpha^n \rfloor \), 33
constructibility
  of regular 17-gon, 45, 56, 78
  of regular \( n \)-gon (Gauss–Wantzel characterization), 46, 55
  rudiments, 50
constructible number, 51, 77
cubic reciprocity law (Eisenstein), 75
cubic reciprocity law (Jacobi), 50, 64, 70, 82
  form of Z.-H. Sun, 73
cubic residuacity
Index

character of 2, 47, 68, 83
character of 3, 69, 83
Cunningham-Gosset criterion, 75
cyclotomic numbers, 61
determination when $e = 3$, 65
cyclotomic polynomials
definition, 24
form of prime divisors, 25
have integer coefficients, 24
irreducibility, 80
cyclotomy, 46
deficient numbers, 248
density, asymptotic, xiii
Dirichlet $L$-series
nonvanishing at $s = 1$ for complex $\chi$, 128
nonvanishing at $s = 1$ for real $\chi$, 132
Dirichlet characters, 126
modulo 4, 120
orthogonality relations for, 127
Dirichlet series, 5, 221
Dirichlet’s theorem, 23, 119
for progressions modulo 4, 120
distribution function, 268
Erdős–Wintner theorem, 268
for $\sigma(n)/n$, 252, 259, 273, 274
divisor function, 114
dual group, 125
Elliott–Halberstam conjecture, 109
Erdős–Kac theorem, 112
Erdős–Straus conjecture, 174, 207
Erdős–Wintner theorem, 268
Euler factorization, 5
Euler’s prime-producing polynomial, 14
Extended Riemann Hypothesis, 143
Farey fraction, 145
Fermat number, 29
Fibonacci number, 203
Gauss sum, 81, 146
Gauss–Wantzel theorem, see also
constructibility of regular $n$-gon
(Gauss–Wantzel characterization)
Gaussian period, 54
period polynomial, 57
form of prime divisors (Kummer’s
criterion), 59
form when $e = 2$, 61
form when $e = 3$, 64
has integer coefficients and is
irreducible, 58
reduced period polynomial, 57
form when $e = 2$, 61
form when $e = 3$, 68
Gelfond–Schneider transcendence theorem, 33
Goldbach conjecture
lower bound on the number of
representations as a sum of almost
primes, 196
quantitative form, 103, 209
upper bound on the number of
representations, 185
Hasse–Minkowski theorem, 140
Hilbert–Dress identities, 152
Hilbert–Waring theorem, 151
Hypothesis H, 27, 28
quantitative form, 103
implied constant, xiii
Jacobson radical, 37
Legendre’s theorem on diagonal ternary
quadratic forms, 135
Linnik’s theorem on the least prime in a
progression, 143
little-oh notation, xii, xiii
logarithmic integral, 86
Möbius inversion, 218
Mann’s theorem, 198
Mann–Shanks primality criterion, 43
Matijasevich–Putnam theorem, 32
Mersenne number, 29
Mersenne prime, 29
Mertens’ theorems, 95
Mertens’ first theorem, 96
Mertens’ second theorem, 97
second theorem for arithmetic
progressions, 141
second theorem for polynomials, 116
multiplication table, 112
multiply perfect number, 272
normal number, 34
normal number of prime factors
of $p - 1$, 207
of a natural number, 111
O and o notation, xiii
Pólya–Vinogradov inequality, 146
perfect numbers, 174, 248
conjectured number up to $x$, 249
Dickson’s theorem, 250
generalization by Kanold, 267
proof of, 253
Euclid–Euler classification of even
perfect numbers, 248
Euler's form of odd perfect numbers, 250
heuristic argument suggesting only
finitely many odd examples, 258
Wirsing's theorem, 251, 267
proof of, 255
polygonal number theorem, 148
prime number graph, 111
prime number theorem
as a consequence of the Wiener–Ikehara
theorem, 214
discovery by Gauss, 86
equivalence to the nonvanishing of \( \zeta(s) \)
on \( \Re(s) = 1 \), 215, 238
equivalent forms in terms of \( \theta \) and \( \psi \), 90
error term, 105
for arithmetic progressions, 101, 240, 245
for polynomials, 115
prime numbers
definition, 1
divergence of reciprocal sum, 7, 10, 173
Fermat prime, 30
have density zero, 88
heuristics from probability, 100
infinite
Braun, Métrod, 2
Erdős, 10
Euclid, 2
Euler (1st proof), 7
Euler (2nd proof), 2
Furstenberg, 12
Goldbach, 3
Hacks, 8, 36
Hemminger, 4
Perott, 9
Saidak, 4
Stieltjes, 2
Washington, 13
Wunderlich, 4
Mersenne prime, 29, 103, 249
of the form \( \frac{1}{2}(n^2 + 1) \), 42
of the form \( [\alpha^n] \), 33
of the form \( n \cdot 2^n + 1 \), 203
of the form \( n^2 + 1 \), 28, 172
of the form \( n^2 + k \), 110
polynomial with prime positive range, 32
prime producing machine, 13
principle of inclusion-exclusion, 170
pseudoperfect number, 276
quadratic reciprocity, 46
cyclotomic proof, 61, 63
first supplementary law, 63
second supplementary law, 64
Rabinowitsch's theorem, 15
random sieve (Hawkins), 104
Riemann Hypothesis, 105
connection with large values of \( \sigma(n) \), 269
Riemann zeta function
continuation to \( \Re(s) > 0 \), 214
definition, 5
Euler factorization, 5
evaluation of \( \zeta(2) \) and \( \zeta(4) \), 35
nonvanishing on \( \Re(s) = 1 \), 238
Romanov's theorem, 210
Schnirelmann density, 197
Schnirelmann's theorem, 196
Selberg's fundamental formula, 215
for arithmetic progressions, 241
proof of, 221
set of multiples, 276
sieve of Eratosthenes, 163
sieve of Eratosthenes–Legendre, 169
application to estimating \( \pi(x) \), 165
general version, 170
Legendre's formula, 164
sign changes of \( \pi(x) - \text{Li}(x) \), 106
smooth numbers, 11, 115
sociable numbers, 253, 263
distribution of, 253, 266
squarefull number, 36, 145
sums of three primes, 201
sums of three squares, 134
number of representations, 140
sums of two squares (number of
representable integers), 174
superperfect number, 270
them there hills, xi
twin primes, 27
convergence of reciprocal sum, 168, 179
infinite of almost prime pairs, 168, 196
twin prime conjecture (qualitative), 27
twin prime conjecture (quantitative), 102
twin prime conjecture for polynomials,
116
untouchable number, 272
Vinogradov's three primes theorem, 201
Waring's problem, 151
determination of \( g(k) \), 161
finiteness of \( g(k) \), 152
upper bound on \( G(k) \), 162
weird number, 277
Wiener–Ikehara theorem, 214
zeta function, see also Riemann zeta function
Number theory is one of the few areas of mathematics where problems of substantial interest can be fully described to someone with minimal mathematical background. Solving such problems sometimes requires difficult and deep methods. But this is not a universal phenomenon; many engaging problems can be successfully attacked with little more than one’s mathematical bare hands. In this case one says that the problem can be solved in an elementary way. Such elementary methods and the problems to which they apply are the subject of this book.

*Not Always Buried Deep* is designed to be read and enjoyed by those who wish to explore elementary methods in modern number theory. The heart of the book is a thorough introduction to elementary prime number theory, including Dirichlet’s theorem on primes in arithmetic progressions, the Brun sieve, and the Erdös–Selberg proof of the prime number theorem. Rather than trying to present a comprehensive treatise, Pollack focuses on topics that are particularly attractive and accessible. Other topics covered include Gauss’s theory of cyclotomy and its applications to rational reciprocity laws, Hilbert’s solution to Waring’s problem, and modern work on perfect numbers.

The nature of the material means that little is required in terms of prerequisites: The reader is expected to have prior familiarity with number theory at the level of an undergraduate course and a first course in modern algebra (covering groups, rings, and fields). The exposition is complemented by over 200 exercises and 400 references.