Graduate Texts in
Mathematics

177

Analytic Number Theory

Springer-Verlag

Graduate Texts
in Mathematics

Donald J. Newman

Analytic Number Theory

Springer

Donald J. Newman
National Security Agency
Fort Meade, MD 20755
USA

Mathematics Subject Classification (1991): 15A60, 65F35, 15A51

Library of Congress Cataloging-in-Publication Data
Newman, Donald J., 1930–
Analytic number theory / Donald J. Newman.
p. cm. — (Graduate texts in mathematics ; 177)
Includes index.
ISBN 0-387-98308-2 (hardcover : alk. paper)
1. Number Theory. I. Title. II. Series.
QA241.N48 1997
512.'73—dc21 97-26431

Printed on acid-free paper.

Production managed by Allan Abrams; manufacturing supervised by Jeffrey Taub.
Photocomposed pages prepared from the author's LaTeX files.
Printed and bound by Edwards Brothers, Inc., Ann Arbor, MI.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-98308-2 Springer-Verlag New York Berlin Heidelberg SPIN 10635124

Graduate Texts in Mathematics 177

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Graduate Texts in Mathematics

1 Takeuti/Zaring. Introduction to Axiomatic Set Theory. 2nd ed.
2 Oxtoby. Measure and Category. 2nd ed.
3 Schaefer. Topological Vector Spaces.
4 Hilton/Stammbach. A Course in Homological Algebra. 2nd ed.
5 Mac Lane. Categories for the Working Mathematician.
6 Hughes/Piper. Projective Planes.
7 Serre. A Course in Arithmetic.
8 Takeuti/Zaring. Axiomatic Set Theory.
9 Humphreys. Introduction to Lie Algebras and Representation Theory.
10 Cohen. A Course in Simple Homotopy Theory.
11 Conway. Functions of One Complex Variable I. 2nd ed.
12 Beals. Advanced Mathematical Analysis.
13 Anderson/Fuller. Rings and Categories of Modules. 2nd ed.
14 Golubitsky/Guillemin. Stable Mappings and Their Singularities.
15 Berberian. Lectures in Functional Analysis and Operator Theory.
16 Winter. The Structure of Fields.
17 Rosenblatt. Random Processes. 2nd ed.
18 Halmos. Measure Theory.
19 Halmos. A Hilbert Space Problem Book. 2nd ed.
20 Husemoller. Fibre Bundles. 3rd ed.
21 Humphreys. Linear Algebraic Groups.
22 Barnes/Mack. An Algebraic Introduction to Mathematical Logic.
23 Greub. Linear Algebra. 4th ed.
24 Holmes. Geometric Functional Analysis and Its Applications.
25 Hewitt/Stromberg. Real and Abstract Analysis.
26 Manes. Algebraic Theories.
27 Kelley. General Topology.
28 Zariski/Samuel. Commutative Algebra. Vol.I.
29 Zariski/Samuel. Commutative Algebra. Vol.II.
30 Jacobson. Lectures in Abstract Algebra I. Basic Concepts.
31 Jacobson. Lectures in Abstract Algebra II. Linear Algebra.
32 Jacobson. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 Hirsch. Differential Topology.
34 Spitzer. Principles of Random Walk. 2nd ed.
35 Wermer. Banach Algebras and Several Complex Variables. 2nd ed.
36 Kelley/Namioka et al. Linear Topological Spaces.
37 Monk. Mathematical Logic.
38 Grauert/Fritzsche. Several Complex Variables.
39 Arveson. An Invitation to C^*-Algebras.
40 Kemeny/Snell/Knapp. Denumerable Markov Chains. 2nd ed.
41 Apostol. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 Serre. Linear Representations of Finite Groups.
43 Gillman/Jerison. Rings of Continuous Functions.
44 Kendig. Elementary Algebraic Geometry.
45 Loève. Probability Theory I. 4th ed.
46 Loève. Probability Theory II. 4th ed.
47 Moise. Geometric Topology in Dimensions 2 and 3.
48 Sachs/Wu. General Relativity for Mathematicians.
49 Gruenberg/Weir. Linear Geometry. 2nd ed.
50 Edwards. Fermat's Last Theorem.
51 Klingenberg. A Course in Differential Geometry.
52 Hartshorne. Algebraic Geometry.
53 Manin. A Course in Mathematical Logic.
54 Graver/Watkins. Combinatorics with Emphasis on the Theory of Graphs.
55 Brown/Pearcy. Introduction to Operator Theory I: Elements of Functional Analysis.
56 Massey. Algebraic Topology: An Introduction.
57 Crowell/Fox. Introduction to Knot Theory.
58 Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 Lang. Cyclotomic Fields.
60 Arnold. Mathematical Methods in Classical Mechanics. 2nd ed.

continued after index

Donald J. Newman

Analytic Number Theory

Springer

Introduction and Dedication

This book is dedicated to Paul Erdös, the greatest mathematician I have ever known, whom it has been my rare privilege to consider colleague, collaborator, and dear friend.

I like to think that Erdös, whose mathematics embodied the principles which have impressed themselves upon me as defining the true character of mathematics, would have appreciated this little book and heartily endorsed its philosophy. This book proffers the thesis that mathematics is actually an easy subject and many of the famous problems, even those in number theory itself, which have famously difficult solutions, can be resolved in simple and more direct terms.

There is no doubt a certain presumptuousness in this claim. The great mathematicians of yesteryear, those working in number theory and related fields, did not necessarily strive to effect the simple solution. They may have felt that the status and importance of mathematics as an intellectual discipline entailed, perhaps indeed required, a weighty solution. Gauss was certainly a wordy master and Euler another. They belonged to a tradition that undoubtedly revered mathematics, but as a discipline at some considerable remove from the commonplace. In keeping with a more democratic concept of intelligence itself, contemporary mathematics diverges from this somewhat elitist view. The simple approach implies a mathematics generally available even to those who have not been favored with the natural endowments, nor the careful cultivation of an Euler or Gauss.

Such an attitude might prove an effective antidote to a generally declining interest in pure mathematics. But it is not so much as incentive that we proffer what might best be called "the fun and games" approach to mathematics, but as a revelation of its true nature. The insistence on simplicity asserts a mathematics that is both "magical" and coherent. The solution that strives to master these qualities restores to mathematics that element of adventure that has always supplied its peculiar excitement. That adventure is intrinsic to even the most elementary description of analytic number theory.

The initial step in the investigation of a number theoretic item is the formulation of "the generating function". This formulation inevitably moves us away from the designated subject to a consideration of complex variables. Having wandered away from our subject, it becomes necessary to effect a return. Toward this end "The Cauchy Integral" proves to be an indispensable tool. Yet it leads us, inevitably, further afield to all the intricacies of contour integration and they, in turn entail the familiar processes, the deformation and estimation of these contour integrals.

Retracing our steps we find that we have gone from number theory to function theory, and back again. The journey seems circuitous, yet in its wake a pattern is revealed that implies a mathematics deeply inter-connected and cohesive.

Contents

I

The Idea of Analytic Number Theory

The most intriguing thing about Analytic Number Theory (the use of *Analysis*, or *function theory*, in number theory) is its very existence! How could one use properties of continuous valued functions to determine properties of those most discrete items, the integers. Analytic functions? What has differentiability got to do with counting? The astonishment mounts further when we learn that the complex zeros of a certain analytic function are *the* basic tools in the investigation of the primes.

The answer to all this bewilderment is given by the two words *generating functions*. Well, there are answers and answers. To those of us who have witnessed the use of generating functions this is a kind of answer, but to those of us who haven't, this is simply a restatement of the question. Perhaps the best way to understand the use of the analytic method, or the use of generating functions, is to see it in action in a number of pertinent examples. So let us take a look at some of these.

Addition Problems

Questions about addition lend themselves very naturally to the use of generating functions. The link is the simple observation that adding m and n is isomorphic to multiplying z^m and z^n. Thereby questions about the addition of integers are transformed into questions about the multiplication of polynomials or power series. For example, Lagrange's beautiful theorem that every positive integer is the sum of four squares becomes the statement that all of the coefficients of the power series for $\left(1 + z + z^4 + \cdots + z^{n^2} + \cdots\right)^4$ are positive. How one proves such a fact about the coefficients of such a power series is another story, but at least one begins to see how this transition from integers to analytic functions takes place. But now let's look at some addition problems that we *can* solve completely by the analytic method.

Change Making

How many ways can one make change of a dollar? The answer is 293, but the problem is both too hard and too easy. Too hard because the available coins are so many and so diverse. Too easy because it concerns just one "change," a dollar. More fitting to our spirit is the following problem: How many ways can we make change for *n* if the coins are 1, 2, and 3? To form the appropriate generating function, let us write, for $|z| < 1$,

$$\frac{1}{1-z} = 1 + z + z^{1+1} + z^{1+1+1} + \cdots,$$

$$\frac{1}{1-z^2} = 1 + z^2 + z^{2+2} + z^{2+2+2} + \cdots,$$

$$\frac{1}{1-z^3} = 1 + z^3 + z^{3+3} + z^{3+3+3} + \cdots,$$

and multiplying these three equations to get

$$\begin{aligned}\frac{1}{(1-z)(1-z^2)(1-z^3)}\\ &= (1 + z + z^{1+1} + \cdots)(1 + z^2 + z^{2+2} + \cdots)\\ &\quad \times (1 + z^3 + z^{3+3} + \cdots).\end{aligned}$$

Now we ask ourselves What happens when we multiply out the right-hand side? We obtain terms like $z^{1+1+1+1} \cdot z^2 \cdot z^{3+3}$. On the one hand, this term is z^{12}, but, on the other hand, it is $z^{\text{four1's+one2+two3's}}$ and doesn't this exactly correspond to the method of changing the amount 12 into four 1's, one 2, and two 3's? Yes, and in fact we see that "every" way of making change (into 1's, 2's, and 3's) for "every" n will appear in this multiplying out. Thus if we call $C(n)$ the number of ways of making change for n, then $C(n)$ will be the exact coefficient of z^n when the multiplication is effected. (Furthermore all is rigorous and not just formal, since we have restricted ourselves to $|z| < 1$ wherein convergence is absolute.)

Thus

$$\sum C(n)z^n = \frac{1}{(1-z)(1-z^2)(1-z^3)}, \tag{1}$$

and the generating function for our unknown quantity $C(n)$ is produced. Our number theoretic problem has been translated into a problem about analytic functions, namely, finding the Taylor coefficients of the function $\frac{1}{(1-z)(1-z^2)(1-z^3)}$.

Fine. A well defined analytic problem, but how to solve it? We must resist the temptation to solve this problem by *undoing* the analysis which led to its formulation. Thus the thing *not* to do is expand $\frac{1}{1-z}$, $\frac{1}{1-z^2}$, $\frac{1}{1-z^3}$ respectively into $\sum z^a$, $\sum z^{2b}$,$\sum z^{3c}$ and multiply only to discover that the coefficient is the number of ways of making change for n.

The correct answer, in this case, comes from an *algebraic* technique that we all learned in *calculus*, namely partial fraction. Recall that this leads to terms like $\frac{A}{(1-\alpha z)^k}$ for which we know the expansion explicitly (namely, $\frac{1}{(1-\alpha z)^k}$ is just a constant times the $(k-1)$th derivative of $\frac{1}{(1-\alpha z)} = \sum \alpha^n z^n$).

Carrying out the algebra, then, leads to the partial fractional decomposition which we may arrange in the following form:

$$\frac{1}{(1-z)(1-z^2)(1-z^3)}$$
$$= \frac{1}{6}\frac{1}{(1-z)^3} + \frac{1}{4}\frac{1}{(1-z)^2} + \frac{1}{4}\frac{1}{(1-z^2)} + \frac{1}{3}\frac{1}{(1-z^3)}.$$

Thus, since

$$\frac{1}{(1-z)^2} = \frac{d}{dz}\frac{1}{1-z} = \frac{d}{dz}\sum z^n = \sum(n+1)z^n$$

and

$$\frac{1}{(1-z)^3} = \frac{d}{dz}\frac{1}{2(1-z)^2} = \frac{d}{dz}\sum \frac{n+1}{2}z^n$$
$$= \sum \frac{(n+2)(n+1)}{2}z^n,$$

$$C(n) = \frac{(n+2)(n+1)}{12} + \frac{n+1}{4} + \begin{cases} \frac{1}{4}, & \text{if } n \text{ is even,} \\ \frac{1}{3}, & \text{if } 3|n \end{cases} \tag{2}$$

A somewhat cumbersome formula, but one which can be shortened nicely into

$$C(n) = \left[\frac{n^2}{12} + \frac{n}{2} + 1\right]; \tag{3}$$

where the terms in the brackets mean the greatest integers.

A nice crisp exact formula, but these are rare. Imagine the mess that occurs if the coins were the usual coins of the realm, namely 1, 5, 10, 25, 50, (100?). The right thing to ask for then is an "asymptotic" formula rather than an exact one.

Recall that an *asymptotic* formula $F(n)$ for a function $f(n)$ is one for which $\lim_{n\to\infty}\frac{f(n)}{F(n)} = 1$. In the colorful language of E. Landau, the *relative error* in replacing $f(n)$ by $F(n)$ is *eventually* 0%. At any rate, we write $f(n) \sim F(n)$ when this occurs. One famous such example is Stirling's formula $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$. (Also note that our result (3) can be weakened to $C(n) \sim \frac{n^2}{12}$.)

So let us assume quite generally that there are coins $a_1, a_2, a_3, \ldots, a_k$, where to avoid trivial congruence considerations we will require that there be no common divisiors other than 1. In this generality we ask for an asymptotic formula for the corresponding $C(n)$. As before we find that the generating function is given by

$$\sum C(n)z^n = \frac{1}{(1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_k})}. \tag{4}$$

But the next step, explicitly finding the partial fractional decomposition of this function is the *hopeless* task. However, let us simply look for one of the terms in this expansion, the *heaviest* one. Thus at $z = 1$ the denominator has a k-fold zero and so there will be a term $\frac{c}{(1-z)^k}$. All the other zeros are at roots of unity and, because we assumed no common divisiors, all will be of order lower than k.

Thus, although the coefficient of the term $\frac{c}{(1-z)^k}$ is $c\binom{n+k}{k-1}$, the coefficients of all other terms $\frac{a}{(1-\omega z)^3}$ will be $a\omega^j\binom{n+j}{j-1}$. Since all of these j are less than k, the sum total of all of these terms is negligible compared to our one *heavy* term $c\binom{n+k}{k-1}$. In short $C(n) \sim c\binom{n+k}{k-1}$, or even simpler,

$$C(n) \sim c\frac{n^{k-1}}{(k-1)!}.$$

But, what is c? Although we have deftly avoided the necessity of finding all of the other terms, we cannot avoid this one (it's the whole story!). So let us write

$$\frac{1}{(1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_k})} = \frac{c}{(1-z)^k} + \text{ other terms,}$$

multiply by $(1-z)^k$ to get

$$\frac{1-z}{1-z^{a_1}}\,\frac{1-z}{1-z^{a_2}}\cdots\frac{1-z}{1-z^{a_k}} = c + (1-z)^k \times \text{ other terms,}$$

and finally let $z \to 1$. By L'Hôpital's rule, for example, $\frac{1-z}{1-z^{a_i}} \to \frac{1}{a_i}$ whereas each of the other terms times $(1-z)^k$ goes to 0. The final result is $c = \frac{1}{a_1a_2\cdots a_k}$, and our final asymptotic formula reads

$$C(n) \sim \frac{n^{k-1}}{a_1a_2\cdots a_k(k-1)!}. \qquad (5)$$

Crazy Dice

An ordinary pair of dice consist of two cubes each numbered 1 through 6. When tossed together there are altogether 36 (equally likely) outcomes. Thus the sums go from 2 to 12 with varied numbers of repeats for these possibilities. In terms of our analytic representation, each die is associated with the polynomial $z + z^2 + z^3 + z^4 + z^5 + z^6$. The combined possibilities for the *sums* then are the terms of the *product*

$$\begin{aligned}(z + z^2 + z^3 + z^4 + z^5 + z^6)&(z + z^2 + z^3 + z^4 + z^5 + z^6)\\ &= z^2 + 2z^3 + 3z^4 + 4z^5 + 5z^6 + 6z^7\\ &\quad + 5z^8 + 4z^9 + 3z^{10} + 2z^{11} + z^{12}\end{aligned}$$

The correspondence, for example, says that there are 3 ways for the 10 to show up, the coefficients of z^{10} being 3, etc. The question is Is there any *other* way to number these two cubes with positive integers so as to achieve the very same alternatives?

Analytically, then, the question amounts to the existence of positive integers, $a_1, \cdots, a_6; b_1, \cdots, b_6$, so that

$$\begin{aligned}(z^{a_1} + \cdots + z^{a_6})&(z^{b_1} + \cdots + z^{b_6})\\ &= z^2 + 2z^3 + 3z^4 + \cdots + 3z^{10} + 2z^{11} + z^{12}.\end{aligned}$$

These would be the "Crazy Dice" referred to in the title of this section. They look totally different from ordinary dice but they produce exactly the same results!

So, repeating the question, can

$$\begin{aligned}(z^{a_1} + \cdots + z^{a_6})&(z^{b_1} + \cdots + z^{b_6})\\ &= (z + z^2 + z^3 + z^4 + z^5 + z^6) \qquad (6)\\ &\quad \times (z + z^2 + z^3 + z^4 + z^5 + z^6)?\end{aligned}$$

To analyze this possibility, let us factor completely (over the rationals) this right-hand side. Thus $z + z^2 + z^3 + z^4 + z^5 + z^6 = z\frac{1-z^6}{1-z}(1 + z^3) = z(1 + z + z^2)(1 + z)(1 - z + z^2)$. We conclude from (6) that the "a-polynomial" and "b-polynomial" must consist of these factors. Also there are certain side restrictions. The a's and b's are to be *positive* and so a z factor must appear in both polynomials. The a-polynomial must be 6 at $z = 1$ and so the $(1 + z + z^2)(1 + z)$ factor must appear in it, and similarly in the b-polynomial. All that is left to distribute are the two factors of $1 - z + z^2$. If one apiece are given to the a- and b- polynomials, then we get ordinary dice. The only thing left to try is putting both into the a-polynomial.

This works! We obtain finally

$$\begin{aligned}\sum z^a &= z(1+z+z^2)(1+z)(1-z+z^2)^2\\ &= z+z^2+z^3+z^4+z^5+z^6+z^8\end{aligned}$$

and

$$\sum z^b = z(1+z+z^2)(1+z) = z+2z^2+2z^3+z^4.$$

Translating back, the crazy dice are 1,3,4,5,6,8 and 1,2,2,3,3,4.

Now we introduce the notion of the *representation function*. So, suppose there is a set A of nonnegative integers and that we wish to express the number of ways in which a given integer n can be written as the sum of two of them. The trouble is that we must decide on conventions. Does order count? Can the two summands be equal? Therefore we introduce *three* representation functions.

$$r(n) = \{\#a, a' \in A, n = a + a'\};$$

So here order counts, and they can be equal;

$$r_+(n) = \{\#a, a' \in A, a \le a', n = a + a'\},$$

order doesn't count, and they can be equal;

$$r_-(n) = \{\#a, a' \in A, a < a', n = a + a'\},$$

order doesn't count, and they can't be equal. In terms of the generating function for the set A, namely, $A(z) = \sum_{a\in A} z^a$, we can express the generating functions of these representation functions.

The simplest is that of $r(n)$, where obviously

$$\sum r(n)z^n = A^2(z). \tag{7}$$

To deal with $r_-(n)$, we must subtract $A(z^2)$ from $A^2(z)$ to remove the case of $a = a'$ and then divide by 2 to remove the *order*. So here

$$\sum r_-(n)z^n = \frac{1}{2}[A^2(z) - A(z^2)]. \tag{8}$$