CAMBRIDGE TRACTS IN MATHEMATICS

125

THE HARDY-LITTLEWOOD METHOD

SECOND EDITION

HARDY-LITTLEWOOD 方法

第 2 版

R. C. VAUGHAN

CAMBRIDGE UNIVERSITY PRESS

世界图书出版公司

R. C. VAUGHAN
Professor of Pure Mathematics and EPSRC Senior Fellow
Imperial College, University of London

The Hardy–Littlewood method

Second Edition


CAMBRIDGE
UNIVERSITY PRESS

世界图书出版公司
北京·广州·上海·西安

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge CB2 1RP, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1981
Second edition 1997

Printed in the United Kingdom at the University Press, Cambridge

Typeset in Times 10/12pt

A catalogue record of this book is available from the British Library

Library of Congress cataloguing in publication data

Vaughan, R. C.
The Hardy–Littlewood method/R. C. Vaughan. – 2nd ed.
p. cm – (Cambridge tracts in mathematics; 125)
Includes bibliographical references (p. –) and index.
ISBN 0 521 57347 5
1. Hardy–Littlewood method. I. Title. II. Series.
QA241.V34 1997
512'.74–dc20 96–19434 CIP

ISBN 0 521 57347 5 hardback

This edition of The Hardy-Littlewood Methods by R.C.Vaughan is published by arrangement with the syndicate of the Press of the University of Cambridge, Cambridge, England.

Licensed edition for sale in the People's Republic of China only. Not for export elsewhere.

VN

Preface

There have been two earlier Cambridge Tracts that have touched upon the Hardy–Littlewood method, namely those of Landau, 1937, and Estermann, 1952. However there has been no general account of the method published in the United Kingdom despite the not inconsiderable contribution of English scholars in inventing and developing the method and the numerous monographs that have appeared abroad.

The purpose of this tract is to give an account of the classical forms of the method together with an outline of some of the more recent developments. It has been deemed more desirable to have this particular emphasis as many of the later applications make important use of the classical material.

It would have been useful to devote some space to the work of Davenport on cubic forms, to the joint work of Davenport and Lewis on simultaneous equations, to the work of Rademacher and Siegel that extends the method to algebraic numbers, and to the work of various authors, culminating in the recent work of Schmidt, on bounds for solutions of homogeneous equations and inequalities. However this would have made the tract unwieldy. The interested reader is referred to the Bibliography.

It is assumed that the reader has a familiarity with the elements of number theory, such as is contained in the treatise of Hardy and Wright. Also, in dealing with one or two subjects it is expected that the reader has a working acquaintance with more advanced topics in number theory. Where necessary, reference is given to a standard text on the subject.

The contents of Chapters 2, 3, 4, 5, 9, 10 and 11 have been made the basis of advanced courses offered at Imperial College over a number of years, and could be used as part of any normal post-graduate training in analytic number theory.

Preface to second edition

At the time that the first edition was written, there had been relatively little recent work on the central theory of the Hardy–Littlewood method, namely that surrounding Waring's problem and associated questions. Indeed, the work of Davenport and Vinogradov had taken on the aspect of being written on tablets of stone. This is in complete contrast to the current situation. In the last decade or so there has been a series of important developments in the area. The tract is, therefore, ripe for revision, and the opportunity has been taken to give an introduction to this new material, and especially to the important work of Wooley. Chapter 5 has been extensively rewritten to take account of our new understanding of Vinogradov's mean value theorem, and a completely new chapter has been added to describe the new work on Waring's problem. Fortunately the large bulk of the material has not been superseded and the underlying ideas still play an important rôle in many of the new developments.

Notation

The letter k denotes a natural number, usually with $k \geqslant 2$, and the statements in which ε appear are true for every positive real number ε. The letter p is reserved for prime numbers.

The Vinogradov symbols $\ll$, $\gg$ have their usual meaning, namely that for functions f and g with g taking non-negative real values $f \ll g$ means $|f| \leqslant Cg$ where C is a constant, and if moreover f is also non-negative, then $f \gg g$ means $g \ll f$.

Implicit constants in the O, $\ll$ and $\gg$ notations usually depend on k, s and ε. Additional dependence will be mentioned explicitly.

As usual in number theory, the functions $e(\alpha)$ and $\| \alpha \|$ denote $e^{2\pi i\alpha}$ and $\min_{h \in \mathbb{Z}} |\alpha - h|$ respectively. Occasionally the expression $\min(X, 1/0)$ occurs, and is taken to be X.

The notation $p^r \| n$ is used to mean that p^r is the highest power of p dividing n.

Contents

1

Introduction and historical background

1.1 Waring's problem

In 1770 E. Waring asserted without proof in his *Meditationes Algebraicae* that every natural number is a sum of at most nine positive integral cubes, also a sum of at most 19 biquadrates, and so on. By this it is usually assumed that he believed that for every natural number $k \geqslant 2$ there exists a number s such that every natural number is a sum of at most s kth powers of natural numbers, and that the least such s, say $g(k)$, satisfies $g(3) = 9$, $g(4) = 19$.

It was probably known to Diophantus, albeit in a different form, that every natural number is the sum of at most four squares. The four square theorem was first stated explicitly by Bachet in 1621, and a proof was claimed by Fermat but he died before disclosing it. It was not until 1770 that one was given, by Lagrange, who built on earlier work of Euler. For an account of this theorem see Chapter 20 of Hardy & Wright (1979).

In the 19th century the existence of $g(k)$ was established for many values of k, but it was not until the present century that substantial progress was made. First of all Hilbert (1909*a*, *b*) demonstrated the existence of $g(k)$ for every k by a difficult combinatorial argument based on algebraic identities (see Rieger, 1953*a*, *b*, *c*; Ellison, 1971). His method gives a very poor bound for $g(k)$.

In the early 1920s Hardy and Littlewood introduced an analytic method which has been the basis for numerical work by Dickson, Pillai and others, and has led to an almost complete evaluation of $g(k)$. Since the integer

$$n = 2^k\left[\left(\frac{3}{2}\right)^k\right] - 1$$

is smaller than 3^k it can only be a sum of kth powers of 1 and 2. Clearly the most economical representation is by $[(\frac{3}{2})^k] - 1$ kth powers of 2

and $2^k - 1$ kth powers of 1. Thus

$$g(k) \geqslant 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2. \tag{1.1}$$

It is very plausible that this always holds with equality, and the current state of knowledge is as follows.

It has been shown that when

$$2^k\left\{\left(\frac{3}{2}\right)^k\right\} + \left[\left(\frac{3}{2}\right)^k\right] \leqslant 2^k \tag{1.2}$$

one has

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2 \tag{1.3}$$

but when

$$2^k\left\{\left(\frac{3}{2}\right)^k\right\} + \left[\left(\frac{3}{2}\right)^k\right] > 2^k$$

one has either

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] - 2$$

or

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] - 3$$

according as

$$\left[\left(\frac{4}{3}\right)^k\right]\left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] + \left[\left(\frac{3}{2}\right)^k\right]$$

is equal to 2^k or is larger than 2^k. For the various contributions to the proof of this, see the Bibliography.

Stemmler (1964) has verified on a computer that (1.2) (and so (1.3)) holds whenever $k \leqslant 200\,000$, and this has been extended to 471 600 000 by Kubina and Wunderlich (to appear). Mahler (1957) has shown that if there are any values of k for which (1.2) is false, then there can only be a finite number of such values. No exceptions are known, and unfortunately the method will not give a bound beyond which there are no exceptions.

1.2 The Hardy–Littlewood method

Nearly all the above conclusions have been obtained in the following way. A theoretical argument based on the analytic method of Hardy and Littlewood produces a number C_k such that every natural number larger than C_k is the sum of at most s_k kth powers of natural numbers where s_k does not exceed the expected value of $g(k)$. Then a rather tedious, but often very ingenious, calculation enables a check to be made on all the natural numbers not exceeding C_k.

One of the features of the Hardy–Littlewood method is that it can be adapted to attack many other problems of an additive nature. The method has its genesis in a paper of Hardy & Ramanujan (1918) concerned mainly with the partition function, but also dealing with the representation of numbers as sums of squares.

Let $\mathscr{A} = (a_m)$ denote a strictly increasing sequence of non-negative integers and consider

$$F(z) = \sum_{m=1}^{\infty} z^{a_m} \qquad (|z| < 1)$$

and its sth power

$$F(z)^s = \sum_{m_1=1}^{\infty} \dots \sum_{m_s=1}^{\infty} z^{a_{m_1} + \dots + a_{m_s}} = \sum_{n=0}^{\infty} R_s(n) z^n,$$

where $R_s(n)$ is the number of representations of n as the sum of s members of $\mathscr{A}$. The objective is an estimate for $R_s(n)$, at least when n is large. By Cauchy's integral formula

$$R_s(n) = \frac{1}{2\pi i} \int_{\mathscr{C}} F(z)^s z^{-n-1} \mathrm{d}z$$

where $\mathscr{C}$ is a circle centre 0 of radius ρ, $0 < \rho < 1$.

Hardy and Ramanujan discovered an alternative way of evaluating the integral when $a_m = m^2$. Suppose that $\rho = 1 - \frac{1}{n}$ and that n is large, and write $e(\alpha) = e^{2\pi i \alpha}$. Then the function F has 'peaks' when $z = \rho e(\alpha)$ is 'close' to the point $e(a/q)$ with q 'not too large'. In fact, F has an asymptotic expansion in the neighbourhood of such points, roughly speaking valid when $|\alpha - a/q| \leqslant 1/(q\sqrt{n})$ and $q \leqslant \sqrt{n}$. By Dirichlet's theorem on diophantine approximation every z under consideration is in some such neighbourhood.

The asymptotic expansion takes the form

$$F\left(\rho e\left(\frac{a}{q}+\beta\right)\right)\sim\frac{C}{q}S(q,a)(1-\rho e(\beta))^{-1/2} \tag{1.4}$$

where

$$S(q,a)=\sum_{m=1}^{q} e(am^2/q).$$

This can be seen by dealing first with the case $\beta=0$ by partitioning the squares into residue classes modulo q and then applying partial summation. Thus, for $s\geqslant 5$ one can obtain

$$R_s(n)\sim\mathfrak{S}_s(n)J_s(n) \tag{1.5}$$

where

$$\mathfrak{S}_s(n)=\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-s}S(q,a)^s e(-an/q)$$

and

$$J_s(n)=C^s\int_{-1/2}^{1/2}(1-\rho e(\beta))^{-s/2}\rho^{-n}e(-\beta n)\mathrm{d}\beta.$$

The integral in $J_s(n)$ is quite easy to estimate, and the series $\mathfrak{S}_s(n)$ reflects certain interesting number theoretic properties of the sequence of squares.

The expansion (1.4) corresponds to a singularity of the series F at $e(a/q)$ on its circle of convergence, and in view of this Hardy and Littlewood coined the terms *singular series* and *singular integral* for $\mathfrak{S}_s(n)$ and $J_s(n)$ respectively.

After the First World War, Hardy & Littlewood (1920, 1921) turned their attention to Waring's problem. Unfortunately, when $a_m=m^k$ with $k\geqslant 3$, they could only show that the expansion corresponding to (1.4) holds when

$$q\leqslant n^{1/k-\varepsilon}\quad\text{and}\quad\left|\alpha-\frac{a}{q}\right|\leqslant q^{-1}n^{1/k-\varepsilon-1},$$

and this only accounts for a small proportion of the points z on $\mathscr{C}$. Since $q^{-1}S(q,a)\to 0$ as $q\to\infty$ (for $(a,q)=1$) one might hope that at any rate F is small compared with the trivial estimate $(1-\rho)^{-1/k}=n^{1/k}$ on the remaining z, a hope reinforced by the fact that (αm^k) is uniformly distributed modulo 1 when α is irrational. Indeed, Hardy and

Littlewood were able to show that F is appreciably smaller than $n^{1/k}$ on the remainder of $\mathscr{C}$ by an alternative argument having its origins in Weyl's (1916) fundamental work on the uniform distribution of sequences, the consequent statement about the size of F often being called Weyl's inequality. They further introduced the terms *major arcs* and *minor arcs* to describe the parts of $\mathscr{C}$ where they used the analogue of (1.4) and Weyl's inequality respectively.

Later Vinogradov (1928*a*) introduced a number of notable refinements, one of which was to replace $F(z)$ by the finite sum

$$f(\alpha) = \sum_{m=1}^{N} e(\alpha m^k) \tag{1.6}$$

where

$$N = [n^{1/k}]. \tag{1.7}$$

Now

$$f(\alpha)^s = \sum_{m=1}^{sn} R_s(m, n)e(\alpha m)$$

where $R_s(m,n)$ is the number of representations of m as the sum of s kth powers, none of which exceed n. Thus

$$R_s(m, n) = R_s(m) \quad (m \leqslant n).$$

Then a special case of Cauchy's integral formula, namely the trivial orthogonality relation

$$\int_0^1 e(\alpha h)\mathrm{d}\alpha = \begin{cases} 1 & \text{when } h = 0 \\ 0 & \text{when } h \neq 0 \end{cases} \tag{1.8}$$

gives

$$\int_0^1 f(\alpha)^s e(-\alpha n)\mathrm{d}\alpha = R_s(n). \tag{1.9}$$

It is clear from the discussions above that $g(k)$ is determined by the peculiar demands of a few relatively small exceptional natural numbers. Thus the more interesting problem is that of the estimation of the number $G(k)$, defined for $k \geqslant 2$ to be the least s such that every sufficiently large natural number is the sum of at most s kth powers of natural numbers. It transpires that $G(k)$ is much smaller than $g(k)$ when k is large and this naturally makes its evaluation much more

difficult. In fact the value of $G(k)$ is only known when $k = 2$ or 4, namely

$$G(2) = 4,\ G(4) = 16,$$

the latter result being due to Davenport (1939*c*). Linnik (1943*a*) has shown that $G(3) \leqslant 7$ and Watson (1951) has given an extremely elegant proof of this. When $k > 3$ all the best estimates available at present for $G(k)$ have been obtained via the Hardy–Littlewood method. Even when $k = 3$ the Hardy–Littlewood method can be adapted to give $G(3) \leqslant 7$ (Vaughan, 1986*c*). Chapters 2, 4, 5, 6, 7 and 12 are devoted to the study of $G(k)$.

1.3 Goldbach's problem

In two letters to Euler in 1742, Goldbach conjectured that every even number is a sum of two primes and every number greater than 2 is a sum of three primes. He included 1 as a prime number, and so in modern times Goldbach's conjectures have become the assertions that every even number greater than 2 is a sum of two primes and every odd number greater than 5 is a sum of three primes.

Hardy & Littlewood (1923*a*,*b*) discovered that their method could also be applied with success to these problems, provided that they assumed the generalized Riemann hypothesis. Thus they were able to show conditionally that every large odd number is a sum of three primes and that almost every even number is a sum of two primes.

In 1937, Vinogradov was able to remove the dependence on the generalized Riemann hypothesis, thereby giving unconditional proofs of the above conclusions. This line of attack on Goldbach's problems is investigated in Chapter 3. However, the nature of the primes, and in particular the problem of their distribution in arithmetic progressions, means that the further refinements of the method (see Montgomery & Vaughan, 1975) are better viewed in the context of multiplicative number theory and have therefore been omitted from this tract.

For many generalizations of the methods described in Chapter 3 see Hua's (1965) monograph.

1.4 Other problems

The last thirty years have seen a large expansion and diversity of the applications of the method, and in Chapters 8, 9, 10, 11 a number of topics have been chosen to illustrate this development. The applications described there, particularly in Chapters 9 and 11 to general forms and inequalities respectively, cover only a small part of the work which has been undertaken in these areas, and should be viewed as an introduction to the original papers listed in the Bibliography.

1.5 Exercises

1 Show that the number $\rho(n)$ of solutions of the equation

$$x_1 + \ldots + x_s = n$$

in non-negative integers $x_1, \ldots, x_s$ is $(-1)^n\binom{-s}{n}$.

2 Show that the sum of the divisors of n, $\sigma(n) = \sum_{m|n} m$, satisfies

$$\sigma(n) = \frac{\pi^2}{6} n \sum_{q=1}^{\infty} q^{-2} c_q(n)$$

where $c_q(n)$ is Ramanujan's sum, i.e.

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q).$$

3 Let P,Q denote real numbers with $P > 1$, $Q \geqslant 2P$. Show that the intervals

$$\{\alpha : |\alpha - a/q| \leqslant q^{-1}Q^{-1}\}$$

with $q \leqslant P$ and $(a,q) = 1$ are pairwise disjoint.

2

The simplest upper bound for $G(k)$

2.1 The definition of major and minor arcs

The introduction of various refinements over the years, most notably by Hua (1938*b*) has led to a simple proof that $G(k) \leqslant 2^k + 1$ which nevertheless illustrates many of the salient features of the Hardy–Littlewood method.

There is a good deal of latitude in the definition of major and minor arcs, and the choice made here is fairly arbitrary.

Let n be large, suppose that N is given by (1.7) and that

$$\nu = \frac{1}{100}, \quad P = N^{\nu}, \tag{2.1}$$

and let δ denote a sufficiently small positive number depending only on k. When $1 \leqslant a \leqslant q \leqslant P$ and $(a,q) = 1$, let

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \leqslant N^{\nu - k}\}. \tag{2.2}$$

The $\mathfrak{M}(q, a)$ are called, for the historical reasons outlined above, the *major arcs*, although in fact they are intervals. Let $\mathfrak{M}$ denote the union of the $\mathfrak{M}(q, a)$. It is convenient to work on the unit interval

$$\mathscr{U} = (N^{\nu - k}, 1 + N^{\nu - k}] \tag{2.3}$$

rather than $(0, 1]$. This avoids any difficulties associated with having only 'half major arcs' at 0 and 1. Observe that $\mathfrak{M} \subset \mathscr{U}$. The set $\mathfrak{m} = \mathscr{U} \setminus \mathfrak{M}$ forms the *minor arcs*.

When $a/q \neq a'/q'$ and $q, q' \leqslant N^{\nu}$, one has

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geqslant \frac{1}{qq'} > \left(\frac{1}{q} + \frac{1}{q'}\right) N^{\nu - k}.$$

Thus the $\mathfrak{M}(q, a)$ are pairwise disjoint.

By (1.9) (for brevity the suffix s is dropped)

$$R(n) = \int_{\mathfrak{M}} f(\alpha)^s e(-\alpha n) \mathrm{d}\alpha + \int_{\mathfrak{m}} f(\alpha)^s e(-\alpha n) \mathrm{d}\alpha \tag{2.4}$$

where $f(\alpha)$ is given by (1.6). Before proceeding with the estimation of these integrals it is necessary to establish some auxiliary lemmas.