HARDY'S LEGACY TO NUMBER THEORY

R. C. VAUGHAN

Communicated by W. W. L. Chen

Abstract

Ths is an expanded version of two lectures given at the conference held at Sydney University in December 1997 on the 50th anniversary of the death of G. H. Hardy.

1991 *Mathematics subject classification (Amer. Math. Soc.)*: 01A60, 11F11, 11M26, 11N35, 11P05, 11P32, 11P55, 11P82.

1. Introduction

The most influential figure in British mathematics this century was undoubtedly G. H. Hardy. It is now almost exactly fifty years since his death, and so it would seem to be most timely to review the many consequences of this influence. Hardy's early work was on the evaluation of integrals and his basic training was as an analyst, indeed Britain's first analyst of note. He was responsible almost single handedly for dragging British mathematics into the twentieth century, for modernising the syllabi at both Cambridge and Oxford, and for founding the very vibrant British school of classical analysis. During the first decade of the century he also started to take an interest in number theory, largely in association with his younger colleague J. E. Littlewood, but also, all too briefly, with S. Ramanujan. He and Littlewood also founded the British school of analytic number theory which to this day is still one of the leading groups in the world in this area.

It would be most remiss not to mention also another aspect of Hardy's legacy, namely expository textbooks. His 1908 'Pure Mathematics' [36] was the first textbook in English on analysis, and, in spite of style and content designed for the student with

a more formal or 'old fashioned' background, was still a standard recommended text when the author arrived at University in 1963. Even more celebrated perhaps is the elementary number theory text, [57] known universally as 'Hardy and Wright', which is still a standard text, especially with regard to those topics which have a more analytic flavour.

Hardy, either singly or jointly, wrote about 60 research papers in number theory, most of them substantial and influential. Many are seminal. They can be classified into two groups. There are those in which the conclusions are either definitive, or where the state of knowledge has not since been further advanced, and there are those which have stimulated a flood of developments and new ideas and applications. In either case one has the impression that Hardy had a fine instinct for what was likely to be of central importance. The bulk of the papers are either in multiplicative number theory or in additive number theory and it is convenient largely to follow this classification. In some instances, such as the work on Goldbach's problem, the areas overlap.

2. Multiplicative number theory

Hardy's first paper on the Riemann zeta function, which is defined for Re $s > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

was an announcement in 1914 in the Comptes Rendus [37] of a proof that this function has infinitely many zeros on the critical line, Re$s = \frac{1}{2}$. The Riemann zeta function has a meromorphic continuation to the whole plane and is analytic at every point except 1 where it has a simple pole with residue 1. Hardy's result can be thought of as a first step towards the still unproved Riemann Hypothesis that all the non-real zeros $\beta + i\gamma$ of $\zeta(s)$ satisfy $\beta = \frac{1}{2}$. By the way, in the author's opinion, the Riemann Hypothesis and its generalisations are now the most important unsolved problems in mathematics. Later in 1918, jointly with Littlewood [41], he obtained the explicit lower bound

$$N_0(T) > T^{\frac{3}{4}-\varepsilon} \quad (T > T_0(\varepsilon))$$

for $N_0(T)$, the number of such zeros $\frac{1}{2} + i\gamma$ with $0 < \gamma < T$, and this was further improved [45] to

$$N_0(T) > KT \quad (T > T_0)$$

and

$$N_0(T + T^{\alpha}) - N_0(T) > KT^{\alpha} \quad (T > T_0)$$

where $\alpha > \frac{1}{2}$ and K is a suitable positive constant.

Selberg [102] refined the method by introducing the important idea of multiplying $\zeta(s)$ by a 'mollifier', essentially the square of the partial sums of the Dirichlet series for $\zeta(s)^{-1/2}$, in order to control better the size of certain mean values, and thereby obtained a lower bound of the correct order of magnitude

$$N_0(T) > KT \log T \quad (T > T_0),$$

although the constant K in this method is very small. Then, in the 1970s, Levinson [73] introduced a somewhat different method which gives $K = 0.342$. The idea is to relate the distribution of zeros of $\zeta(s)$ to those of $\zeta'(s)$ via the logarithmic derivative of the functional equation. There have been a number of further refinements of Levinson's method by Levinson [74, 75], by Lou [78], and by Conrey [12] who obtained $K = 0.3658$.

The 1918 paper of Hardy and Littlewood quoted above is a gold mine of theorems on the Riemann zeta-function and the distribution of primes, some of them on the assumption of the Riemann Hypothesis. The results were new then of course, but are now routinely assumed and taken for granted as the starting point for further investigations. For example, it is there that the important mean value

(2.1) $$\int_{-T}^{T} \left| \zeta\left(\frac{1}{2} + it\right) \right|^2 dt \sim 2T \log T$$

is first established. Another example, this time on the assumption of the Riemann Hypothesis, is the conclusion that

$$\sum_p x^p \log p = \frac{1}{1-x} + O\left((1-x)^{-\frac{1}{2}}\right)$$

as $x \to 1-$ which, for example, Montgomery and the author [84] were able to make good use of to show in the ternary Goldbach problem that there is some limitation on the quality of the approximation in the asymptotic formula for the number of representations of a number as the sum of three primes. This problem will be returned to below and discussed in greater detail.

A hypothesis which can sometimes serve in place of the Riemann Hypothesis, and which would follow from it, is the Lindelöf Hypothesis, which says that for any real number σ, for every positive real number ε, for each sufficiently large t,

$$|\zeta(s)| < |t|^{\max\left(\frac{1}{2}-\sigma,0\right)+\varepsilon}$$

where $s = \sigma + it$. In a remarkable paper in which the results are still definitive and the theory has not moved on much further, Hardy and Littlewood [48], obtain eight

equivalent assertions to the Lindelöf Hypothesis. Perhaps the most interesting of these is a criterion involving moments, namely that for each $k = 1, 2, 3, \ldots$ and for each $\varepsilon > 0$,

$$\frac{1}{T} \int_1^T \left| \zeta\left(\frac{1}{2} + it\right) \right|^{2k} dt = O(T^\varepsilon).$$

In a connected paper, [46], they obtain the important bound

(2.2)
$$\int_{-T}^T \left| \zeta\left(\frac{1}{2} + it\right) \right|^4 dt = O(T(\log T)^4).$$

This, together with (2.1), is an important ingredient in modern work on the distribution of the zeros of $\zeta(s)$, and in particular for upper bounds for $N(\sigma, T)$ the number of real zeros $\beta + i\gamma$ of $\zeta(s)$ with $\beta > \sigma$ and $0 < \gamma \leq T$. The method of proof of (2.2) is via something called the approximate functional equation. In essence this says that although the Dirichlet series defining $\zeta(s)$ diverges when $\sigma \leq 1$, if one takes a suitable partial sum of this series it is still quite a good approximation to $\zeta(s)$ in the critical strip. In [53] the form of this approximation is obtained which is still the best that is known, namely that when $s = \sigma + it, 0 < \sigma < 1$, one has

$$\zeta(s) = \sum_{n \leq x} \frac{1}{n^s} + \chi(s) \sum_{n \leq y} \frac{1}{n^{1-s}} + O\left(x^{-\sigma} + |t|^{\frac{1}{2} - \sigma} y^{\sigma - 1}\right)$$

where

$$\chi(s) = \pi^{s - \frac{1}{2}} \frac{\Gamma\left(\frac{1}{2} - \frac{1}{2}s\right)}{\Gamma\left(\frac{1}{2}s\right)}.$$

It is quite remarkable how much of Hardy's work in this area is still definitive. But Hardy also contributed to the area through his lectures and his leadership. In particular a number of gifted students were attracted to work in the area, and one of them, Titchmarsh [109], produced what is still the standard text on the Riemann zeta-function.

3. Joint work with Ramanujan

Perhaps Hardy's most famous contribution to mathematics was his support for Ramanujan, and the affect this has had on number theory and the theory of modular forms. One joint paper which stimulated a good deal of later work and developments was [56] in which it is shown that $\omega(n)$, the number of distinct prime factors of n, has normal order $\log \log n$, more precisely that given any function $f(n)$ satisfying

$f(n) \to \infty$ as $n \to \infty$ one has $|\omega(n) - \log\log n| < f(n)\sqrt{\log\log n}$ for almost all n. Their proof follows from a study of the distribution of those n for which $\omega(n)$ has a given value k. This result suggests that $\omega(n)$ is rather well distributed, and that it should have a distribution function. A first step in this direction was taken by Turán [111] who established the inequality

$$\sum_{n \leq x} |\omega(n) - \log\log n|^2 = O\left(x\log\log x\right).$$

His proof is very short and only depends in a straightforward way on simple elementary results in the theory of distribution of primes. In fact with very little further elaboration one can obtain the Turán-Kubilius inequality (Kubilius [72]), that for each positive number ε there is an $x_0(\varepsilon)$ such that for every $x > x_0(\varepsilon)$ one has for any additive function $f(n)$

$$x^{-1} \sum_{n \leq x} |f(n) - A(x)|^2 \leq (2 + \varepsilon)B(x)^2,$$

where

$$A(x) = \sum_{p^k \leq x} \frac{f(p^k)}{p^k}(1 - p^{-1})$$

and

$$B(x)^2 = \sum_{p^k \leq x} \frac{|f(p^k)|^2}{p^k}.$$

A little later Erdős and Kac [29, 30] were able to show that $\omega(n)$ has essentially a normal distribution about its mean. This is the genesis of probabilistic number theory, and since then the techniques and ideas which have flowed across a broad landscape have created a host of important and vital weapons in the research armoury of analytic number theorists. There are several modern texts which give an excellent oversight of this area by Elliott [24–26] and Tenenbaum [108].

Perhaps the most cited of Hardy's papers in number theory is the joint one with Ramanujan [55] on $p(n)$, the number of ways of writing n as the sum of any number of positive integers. Thus

$$6 = 5 + 1 = 4 + 2 = 3 + 3 = 4 + 1 + 1$$
$$= 3 + 2 + 1 = 3 + 1 + 1 + 1 = 2 + 2 + 2$$
$$= 2 + 2 + 1 + 1 = 2 + 1 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 + 1$$

and so $p(6) = 11$. They obtain an asymptotic formula for $p(n)$ of such a precision that it could be used for calculating $p(n)$. Later, of course, Rademacher [87], refined the method to obtain the exact formula

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{q=1}^{\infty} \sqrt{q} A_q(n) \frac{d}{dn} \left(\frac{\sinh\left(\frac{\pi}{q}\sqrt{\frac{2}{3}}\sqrt{n - \frac{1}{24}}\right)}{\sqrt{n - \frac{1}{24}}} \right),$$

where

$$A_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e^{i\pi s(a,q)} e(-an/q)$$

and $s(a, q)$ is Dedekind's sum

$$s(a, q) = \sum_{b=1}^{q-1} \frac{b}{q} \left(\left(\frac{ab}{q} \right) \right),$$

$((x)) = x - [x] - \frac{1}{2}$ when x is not an integer and is 0 otherwise, and $e(z) = e^{2\pi i z}$. There is a very interesting article by Selberg [103] reflecting on the relationship between Hardy and Ramanujan, and giving an excellent insight into this work. The underlying idea behind the proof has been enormously influential. The starting point is the generating function

$$f(z) = \prod_{k=1}^{\infty} (1 - z^k)^{-1} = 1 + \sum_{n=1}^{\infty} p(n) z^n,$$

which converges when $|z| < 1$. Now an identity of Euler shows that

$$z^{1/24} f(z)^{-1} = \sum_{k=-\infty}^{\infty} (-1)^k z^{(6k-1)^2/24},$$

which is a theta function, and by the usual linear fractional transformations one finds when

$$(a, q) = 1, \quad aa' \equiv -1 \pmod{q}, \quad w = u + iv, \quad v > 0,$$

that

$$f\left(e\left(\frac{a}{q} + w \right) \right) = \rho(q, a)\sqrt{-qiw} \exp\left(\frac{\pi i}{12} \left(\frac{1}{q^2 w + w} \right) \right) f\left(e\left(\frac{a'}{q} - \frac{1}{q^2 w} \right) \right)$$

where $\rho(q, a)$ is a root of unity. Now if one supposes that w is small, with $\operatorname{Re} w \le \Im w$, then one is studying f on an arc centered near a 'rational point' on the unit circle, and

$$\operatorname{Re} \frac{2\pi i}{q^2 w}$$

is large so that f on the right is dominated by its constant term 1. Thus the other factors on the right give a good approximation to f on this arc. By applying the Cauchy integral formula to f on a circle of centre the origin and of radius just a bit smaller than 1 one can pick out the coefficient $p(n)$. Then by partitioning the circle into a large number of small arcs, using on each one the approximation just described, adding up the contributions from each arc, and letting their number tend to infinity one can obtain the desired formula.

In this paper (Section 7.2) there is also a brief discussion about the representation of a number as the sum of a fixed number of squares of integers. This is the genesis of the celebrated Hardy-Littlewood circle method, and it is on this and related matters that the rest of the lecture is concentrated.

4. Partitio Numerorum: Waring's Problem

Thus if $r_s(n)$ is the number of representations of n as a sum of s squares, then

$$\theta(z)^s = 1 + \sum_{n=1}^{\infty} r_s(n) z^n,$$

where

$$\theta(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + \sum_{n=1}^{\infty} 2z^{n^2}$$

is also a theta function and a similar analysis can be contemplated. The objective is an approximation to $r_s(n)$ when n is large from which one can deduce that it is positive for all large n. By Cauchy's integral formula one has

$$r_s(n) = \frac{1}{2\pi i} \int_{\mathscr{C}} \theta(z)^s z^{-n-1} dz$$

where $\mathscr{C}$ is a circle centre the origin of radius $\rho, 0 < \rho < 1$. Suppose that $z = \rho e(a/q)$, where $(a, q) = 1$ and $e(z) = e^{2\pi i z}$. Then by rearranging the terms of θ according to the residue class of n modulo q one finds that

$$\theta(z) = \sum_{x=1}^{q} e(ax^2/q) \sum_{\substack{n=1 \\ n \equiv x \pmod{q}}}^{\infty} \rho^{n^2}$$

and when ρ is close to 1, by a variant of the integral test, for example, this is readily seen to give

$$\theta(z) \sim q^{-1} S(q, a) C (1 - \rho)^{-1/2}$$

where C is a certain positive constant and $S(q, a)$ is the Gauss sum

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

Moreover one can expect such an expression to be valid for z in a neighbourhood of $\rho e(a/q)$, and as z moves away from this point it is not hard to see by partial summation that to start off with there is some decay and

$$\theta(\rho e(a/q + \beta)) \sim q^{-1} S(q, a) C (1 - \rho e(\beta))^{-1/2}.$$

It is not hard to obtain a quantitative version of this valid roughly whenever

$$z = \rho(a/q + \beta), \quad \rho = 1 - 1/n, \quad |\beta| \le 1/(q\sqrt{n}), \quad q \le \sqrt{n}.$$

Fortunately, by Dirichlet's theorem on diophantine approximation, every point on the circle lies on such an arc and this leads to an asymptotic formula for $r_s(n)$

$$r_s(n) \sim \mathfrak{S}_s(n) J_s(n),$$

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

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

valid whenever $s \ge 5$. The integral in $J_s(n)$ here is quite easy to estimate, and is asymptotically

$$C' n^{s/2-1}$$

and the series $\mathfrak{S}_s(n)$ reflects certain interesting number theoretic properties of the sequence of squares, and can be shown to be bounded below by a positive constant provided $s \ge 5$. Of course, it is already known that four squares suffice (Lagrange,

1770), and, from the work of Jacobi, that the above asymptotic formula holds when $s = 4$, and indeed more strongly as an exact formula. What is interesting about this is the comparative simplicity of the idea and the possibility of applying it to a whole range of problems.

This is what Hardy and Littlewood proceeded to do, with very profound consequences. In doing so they had to make a very important innovation, and this can be best described, perhaps, in relationship to their work on Waring's problem, that is, the question of how large s has to be so that every positive integer can be written as the sum of at most s kth powers of positive integers. Waring (1770, see [124], pp. 336 and 379) had asserted a belief that 4 squares, 9 cubes, 19 biquadrates, and so on, would suffice. A number of special cases had been treated in the nineteenth century, and eventually in 1909 Hilbert [63] had shown that for each k such an s exists, and his method could be made to give an upper bound for s as a function of k. However, this bound grew so rapidly with k that his result has never been viewed as much more than a pure existence theorem. The smallest such s which suffices for a particular k is usually denoted by $g(k)$. It is now believed that

(4.1)
$$g(k) = 2^k + \left[\left(\frac{3}{2} \right)^k \right] - 2,$$

it certainly being true that

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

requires this many summands, and (4.1) is now known to hold whenever $k \le 471,600,000$. Also Mahler [79] has shown that if there are any exceptions, then there are only a finite number of them. The proofs of (4.1) are the combined efforts of many mathematicians, but the seminal work is that of Hardy and Littlewood in a very important series of papers, embarked upon on Littlewood's return from the First World War, 'On some problems of Partitio Numerorum' [42–44, 47, 49–52].

Now write

$$F(z) = \sum_{m=1}^{\infty} z^{m^k} \quad (|z| < 1).$$

Then by collecting together those terms in the multiple sum for which $m_1^k + \cdots + m_s^k = n$ one finds that

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

where $R_s(n)$ is the number of representations on n in the required form $m_1^k + \cdots + m_s^k = n$. Proceeding as for squares one has

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

where $\mathscr{C}$ is a circle centre the origin of radius ρ, $0 < \rho < 1$, and on an arc near the rational point $e(a/q)$ one has an approximation

$$F(\rho e(\beta + a/q)) \sim q^{-1} S(q, a) C_k (1 - \rho e(\beta))^{-1/k}$$

where now $S(q, a)$ is the generalised Gauss sum

$$S(q, a) = \sum_{x=1}^{q} e(ax^k/q).$$

Unfortunately Hardy and Littlewood were only able to establish this when, essentially,

$$\rho = 1 - 1/n, \quad |\beta| < q^{-1} n^{-1+1/k}, \quad 1 \le a \le q \le n^{1/k}, \quad (a, q) = 1$$

and, when $k > 2$, these arcs only cover a negligible proportion of the circle radius ρ. In order to deal with this difficulty, however, they were able to draw upon ideas then recently expounded by Weyl [125] in his seminal work on uniform distribution. They would have realised that if α is not very close to a rational number with a small denominator, then the values of $e(\alpha x^k)$ can be expected to be fairly uniformly distributed around the unit circle and so one might expect that $f(\alpha)$ is small compared with the crude estimate $O(n^{1/k})$ obtained by replacing each term in f by ρ^{m^k}. In fact they were able to make use of some of the techniques introduced by Weyl in order to show that on the remaining arcs the generating function is indeed relatively small. It was in view of the distinction between the two kinds of arcs, those on which one has an asymptotic result and those on which one has only a O-estimate that they coined the terms 'major arcs' and 'minor arcs' respectively, and it is this division which is what one usually has in mind when in speaking of the Hardy-Litlewood method. In this way they were able to obtain [44, 47] the asymptotic formula

$$R_s(n) \sim \mathfrak{S}_s(n) \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} n^{s/k-1}$$

whenever $s \ge (k - 2)2^{k-1} + 5$. Here the 'singular series'

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

reflects the solubility of the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv n \pmod{q}$$

with $(x_i, q) = 1$ for some i (nonsingular solubility). They were able to show that $\mathfrak{S}_s(n)$ is bounded away from zero whenever for every q this congruence has a nonsingular solution. Thus if one defines $G(k)$ to be the smallest s such that every sufficiently large natural number is the sum of at most s kth powers of natural numbers, then their method gave quite effective upper bounds for $G(k)$, and, in particular, gave

$$G(k) \le (k-2)2^{k-1} + 5.$$

There has been a great deal of work on this in the intervening 75 years. There is an important innovation by Vinogradov in which the generating functions $F(z)$ are replaced by finite sums, which can now be studied on the unit circle, thus f becomes

$$f(\alpha) = \sum_{m \le n^{1/k}} e(\alpha m^k).$$

The current state of play on the above asymptotic formula is that it has been shown to hold for $s > 2^k$ by Hua [68], for $s = 2^k$ by Vaughan [115, 116], for $s > 7.2^k/8$ and $k \ge 6$ by Heath-Brown [60, 61], for $s = 7.2^k/8$ and $k \ge 6$ by Boklan [4], and when k is larger than about 10 for $s \ge s_0$ where $s_0 \sim Ck^2 \log k$ by the method of Vinogradov. In its most refined form, by Ford [32], one has $C = 1$.

In the sixth paper of the 'Partitio Numerorum' sequence they introduce a further idea which was another pointer to a great deal of later work. One of the difficulties in gaining control of the minor arcs is a lack of suitably good mean value estimates for $f(z)$, or, with Vinogradov's innovation, for $f(\alpha)$. It turns out that one has much tighter control if there is an efficient way of constructing fairly dense sets $\mathscr{L}_t$ of natural numbers l each one of which is a sum of t kth powers of natural numbers. They introduced a way of doing just that. It is based on the very simple observation that the kth powers are themselves spaced an appreciable distance apart. In particular when $P < m < n < 2P$ one has $n^k - m^k = (n-m)(n^{k-1} + \cdots + m^{k-1}) > kP^{k-1}$. Thus one can construct the $\mathscr{L}_t$ by taking $P_r = 2^{-r} P^{(1-1/k)^{r-1}}$ and considering the numbers l of the form

$$l(\mathbf{m}) = m_1^k + m_2^k + \cdots + m_t^k$$

with $P_r < m_r < 2P_r$. Now they observed that for large P these numbers $l(\mathbf{m})$ are distinct, and actually this is quite easy to see, for suppose that

$$l(\mathbf{m}) = l(\mathbf{n})$$

and let j be the smallest j such that $m_j \neq n_j$. Then

$$kP_j^{k-1} < |m_j^k - n_j^k| \leq |m_{j+1}^k - n_{j+1}^k| + O(P_{j+2}^k) < P_j^{k-1} + O(P_j^{(k-1)(1-1/k)})$$

which is impossible if P, and hence P_j, is large enough. The number of choices of $\mathbf{m}$ is at least $\frac{1}{2}P_1 P_2 \cdots P_t > C P^{k-k(1-1/k)^t}$ and no $l(\mathbf{m})$ exceeds $2^{k+1} P^k$. Thus by taking $P = \frac{1}{3} N^{1/k}$ they were able to construct sets $\mathscr{L}_t \subset [1, N]$ of the required kind which have at least $C N^{1-(1-1/k)^t}$ elements, and for t growing only a bit larger than k the exponent is already quite close to 1. This is the so-called 'diminishing ranges' argument, and whilst it was only used by Hardy and Littlewood to obtain a fairly modest improvement in the above stated upper bound for $G(k)$, it was later taken up very effectively by Vinogradov and Davenport. In fact the state of the art in 1985 was as follows

$$G(4) = 16, \quad G(5) \leq 23, \quad G(6) \leq 36, \quad G(7) \leq 53, \quad G(8) \leq 73$$

the first three by Davenport [14, 15], and the latter two by his methods, and

$$\limsup_{k \to \infty} \frac{G(k)}{k \log k} \leq 2$$

due to Vinogradov [123]. Actually, Davenport was able to show that a function, modified to take account of local solvability, satisfies

$$G^*(4) \leq 14.$$

Here $G^*(4)$ is the smallest number s such that whenever $1 \leq r \leq s$ every sufficiently large number $n \equiv r$ (mod 16) is the sum of at most s biquadrates. Also, it should be pointed out here, that having such relatively good bounds for $G(k)$ means that the determination of $g(k)$ for any given k is only a finite computation(!), and it is indeed via this route that one has the almost complete determination of $g(k)$ when $k \geq 4$ which was mentioned earlier.

There is a variant of the diminishing range technique, which can be thought of as a p-adic version. Suppose, for the purposes of illustrating the idea, that k is odd and consider for a given prime number p with $P^{1/k} < p < 2P^{1/k}$ and $p \equiv -1$ (mod k) those numbers of the form

$$m^k + p^k l$$

where $m \leq P$, $p \nmid m$ and where l belongs to a set $\mathscr{L} \subset [1, 2^{-k} P^{k-1}]$. Again these numbers are distinct because otherwise if $m^k + p^k l = m'^k + p^k l'$, then one would have $m^k \equiv m'^k$ (mod p^k) and since k is coprime to the order of the multiplicative group of residue classes modulo p^k one would have $m \equiv m'$ (mod p^k). But $p^k > P$ so

$m = m'$, and so on. This is more complicated of course, but it gives a chance for more wrinkles in the argument. Already both Davenport and Vinogradov make use of this idea in their work.

All of the diminishing ranges arguments have one fairly big disadvantage. They destroy the homogeneity of the form

$$(4.2) \qquad\qquad m_1^k + \cdots + m_t^k$$

and from an analytic point of view this renders nugatory many of the symmetries one would like to make use of in mean value theorems. However, more recently there has been a further development of this technique [117]. Consider those numbers of the form (4.2) with each m_j belonging to the set $\mathscr{A}(P, P^\varepsilon)$ of natural numbers not exceeding P with no prime factor exceeding P^ε. In Carl Pommerance's slightly tongue-in-cheek parlance this is the set of 'smooth' numbers, of level P^ε. By the way, even in this terminology one sees the influence of Hardy. In one of his lectures [39] on Ramanujan describing the work [89] on highly composite numbers there is a passage in which certain numbers are called round. Well, the smooth numbers are not exactly round, but they are, er, well, sort of round ..., and certainly smooth!

These smooth numbers have a very interesting property. Given $R < P$ and $m \in \mathscr{A}(P, P^\varepsilon)$ with $m > R$ there is always a divisor r of m with $R < r \le RP^\varepsilon$. The point is that one can take successive prime factors from m and multiply them together until one just gets beyond R, and obviously the number r so obtained cannot be larger than RP^ε. Now it turns out that in m^k the factor r^k can be made to play the same rôle as the p^k in the p-adic method. However the retention of a homogeneous structure in (4.2) has enabled us to use a very large range of techniques, and has led to some striking lowering of the upper bounds for $G(k)$. Thus one now has

$$G^*(4) \le 12, \quad G(5) \le 17, \quad G(6) \le 24,$$
$$G(7) \le 33, \quad G(8) \le 42, \quad G(9) \le 51.$$

The first of these is in [117], the third in [120], the fifth in [119], and the rest in [121]. For larger k, Wooley has shown [126] that

$$\limsup_{k\to\infty} \frac{G(k)}{k \log k} \le 1.$$

5. Partitio Numerorum: The Goldbach Problems

Now let me return to 'Partitio Numerorum'. Hardy and Littlewood [49, 50] also turned their attention towards the other famous pair of questions of additive number theory, namely the Goldbach problems, firstly as to whether every even number greater

than 2 is the sum of two primes, and secondly as to whether every odd number greater than 5 is the sum of three primes. Here the natural generating function is

$$F(z) = \sum_p z^p,$$

but for reasons of technical convenience one usually prefers to work with

$$F(z) = \sum_p z^p \log p.$$

Then

$$F(z)^s = \sum_{n=1}^{\infty} R_s(n) z^n,$$

where

$$R_s(n) = \sum_{\substack{p_1,\dots,p_s \\ p_1+\cdots+p_s=n}} \log p_1 \cdots \log p_s.$$

Now one runs into the problem that there is only rather indifferent information about the distribution of primes in arithmetical progressions, and even today one is forced to take the major arcs to be extremely thin. Moreover, Weyl's work sheds no light on the distribution of the sequence αp when α is not well approximated by a rational number with a small denominator, so there was no obvious way to proceed on the minor arcs. Thus Hardy and Littlewood decided to proceed on the basis of the Generalised Riemann Hypothesis (GRH). Let χ be a Dirichlet character modulo q, that is, a homomorphism from the multiplicative group of reduced residue classes modulo q to $\mathbb{C}$. Then the Dirichlet series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

has a meromorphic continuation to the whole of $\mathbb{C}$, and indeed, unless χ is a trivial character it is an entire function. Then the GRH is the statement that all the zeros of $L(s, \chi)$ have their real parts not exceeding $\frac{1}{2}$. With the assumption of this very powerful hypothesis it was possible to treat all the arcs, and this led to an asymptotic formula. In particular, when $s = 3$ they were able to show that

(5.1)

$$\sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 \sim \frac{1}{2} n^2 \prod_{p|n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid n} \left(1 + \frac{1}{(p-1)^3}\right).$$

When $s = 2$, their method was less successful, but they were still able to show that

$$\sum_{n \leq X} \left| R_2(n) - n \prod_{p|n} \left(\frac{p}{p-1} \right) \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2} \right) \right|^2 = O\left(X^{\frac{5}{2}+\varepsilon} \right),$$

and from this it follows that

$$E(X) := \operatorname{card}\{n \leq X : 2|n, R_2(n) = 0\} = \left(X^{\frac{1}{3}+\varepsilon} \right),$$

and in particular that almost every even number is the sum of two primes.

Later, in 1937, Vinogradov [121], using, of course, instead of the F above, the finite sum

$$F(\alpha) = \sum_{p \leq X} e(\alpha p)$$

found a very ingenious way of estimating this sum non-trivially on the minor arcs, and thereby gave an unconditional proof of the asymptotic formula (5.1). Using Vinogradov's results on $F(\alpha)$ a number of authors [11, 13, 31] were able immediately to show that for any fixed positive $A > 0$, $E(X) = O(X(\log X)^{-A})$. More recently Montgomery and Vaughan [86] were able to show that there is a positive number δ such that

$$E(X) = O(X^{1-\delta}).$$

6. Partitio Numerorum: other consequences

This celebrated series of papers had a number of other consequences. One was that for many problems one could use it as a predictive tool. For example in the Goldbach binary problem, or the question as to the solubility, and number of solutions for large n of,

$$n = p + x^2 + y^2,$$

or of

$$n = f(x_1, \ldots, x_k),$$

where f is a form of degree d with integer coefficients, one could predict an asymptotic formula for the number of solutions by first constructing the appropriate generating functions and then working out the contribution from the major arcs, and finally assuming that the contribution from the minor arcs is of smaller order.

One of the papers in the 'Partitio Numerorum' series, number VII, was never published, probably because it also needed to assume the GRH and Hardy and Littlewood felt that that they did not want to publish too much which depended on an unproved hypothesis. This manuscript dealt with small differences between prime numbers. Let $p_1 = 2$, $p_2 = 3, \ldots$ be the sequence of primes. By the prime number theorem,

$$l := \liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 1.$$

Of course, if one believes in the twin prime hypothesis, then $l = 0$. On GRH, they were able to show that $l \leq \frac{2}{3}$ and Rankin [91] showed that the method would give $(1 + 4\Theta)/5$ where Θ is such that no Dirichlet L-function has a zero with real part exceeding Θ, so in particular on GRH, $l \leq \frac{3}{5}$. At about the same time, Erdős [28] gave an unconditional proof that $l < 1$ via Brun's sieve, and later Ricci [93] showed that $l \leq \frac{15}{16}$.

The starting point of PN VII is an observation, which, for simplicity of exposition, is perhaps best cast in a more modern form, namely that the integral

$$\int_0^1 |S(\alpha)|^2 |K(\alpha)|^2 d\alpha$$

where the generating function is

$$S(\alpha) = \sum_{p \leq X} (\log p) e(\alpha p)$$

and there is a kernel formed from

$$K(\alpha) = \sum_{h \leq H} e(\alpha h),$$

counts (with weight $\log p_1 \log p_2 (H - |h|)$) the number of solutions of

$$p_1 - p_2 = h.$$

The contribution from the term $h = 0$ is easily estimated via the prime number theorem and contributes asymptotically

$$H X \log X.$$

Suppose that the major arcs contribute a larger amount. Then since the integrand is positive one can throw the minor arcs away and still deduce that there are primes p_1, p_2 with

$$0 < p_1 - p_2 < H$$

and so the question then is how small can one make H and yet be successful in this endeavour. This was largely the state of play when Bombieri and Davenport [6] started to work on the problem. One thing which is immediately evident when one works on this is that information about the distribution of primes in arithmetic progressions to moduli out to $\sqrt{X}$ would be very useful, and it was about this time that Roth [97] had been working on the large sieve. Thus in order to describe this part of Hardy's legacy it is necessary to go on a small detour to meet the large sieve. It has already been seen in Hardy's work with Ramanujan that it is possible to deal with the normal order of some arithmetical functions and that this was developed by Turán and Kubilius. Linnik [76] and Rényi [92] had also spotted the potential of dealing in a similar way with the general distribution of sequences into residue classes modulo a prime,

$$Z(p, h) = \sum_{\substack{n \leq N \\ n \equiv h \pmod p}} a_n.$$

Here one might hope that the expected value of this is Z/p where

$$Z = \sum_{n \leq N} a_n.$$

By the orthogonality property of the additive characters,

$$Z(p, h) = \frac{1}{p} \sum_{a=1}^{p} e\left(-\frac{ah}{p}\right) \sum_{n \leq N} a_n e\left(\frac{a}{p}n\right)$$

and so

$$\sum_{h=1}^{p} \left| Z(p, h) - \frac{Z}{p} \right|^2 = p^{-1} \sum_{a=1}^{p-1} \left| \sum_{n \leq N} a_n e\left(\frac{an}{p}\right) \right|^2.$$

Thus

$$\sum_{P \leq Q} p \sum_{h=1}^{p} \left| Z(p, h) - \frac{Z}{p} \right|^2 = \sum_{p \leq Q} \sum_{a=1}^{p-1} \left| S\left(\frac{a}{q}\right) \right|^2,$$

where

$$S(\alpha) = \sum_{n=1}^{N} a_n e(\alpha n).$$

Now suppose that there is a $\lambda = \lambda(N, Q)$ such that for every sequence of complex numbers a_n one has

(6.1)
$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \leq \lambda \sum_{n \leq n} |a_n|^2.$$

Moreover, suppose that for each prime p there are $f(p)$ residue classes h for which $Z(p, h) = 0$ and suppose that $a_n = 1$ or 0, so that one can think of Z as counting the elements of a set which have arisen by a sieving process in which $f(p)$ residue classes are removed for each prime modulus p. Then the above gives

$$\sum_{p \leq Q} p^{-1} Z^2 f(p) \leq \lambda Z,$$

that is,

$$Z \leq \frac{\lambda}{\sum_{p \leq Q} p^{-1} f(p)}.$$

The number $f(p)$ of residue classes 'removed' can be large and so for this reason, a nontrivial inequality of the kind (6.1) is known as the large sieve inequality. Actually there are ways of making use of the information from composite q in (6.1) to obtain upper bound sieve estimates [7, 81]

$$Z \leq \frac{\lambda}{\sum_{q \leq Q} \mu(q)^2 \prod_{p|q} \frac{f(p)}{p - f(p)}}$$

which are similar to those obtained by other upper bound sieve methods.

In [97] Roth had obtained the remarkable bound

$$\lambda \leq C(N + Q^2 \log Q),$$

and it turned out that bounds of this kind in (6.1) were just what Bombieri and Davenport needed in their work on small differences between primes. In fact, Bombieri [5] was able to show that

$$\sum_{q \leq x^{1/2}(\log x)^{-B(A)}} \max_{(a,q)=1} \sup_{y \leq x} \left| \sum_{\substack{p \leq y \\ p \equiv a \pmod q}} 1 - \frac{1}{\phi(q)} \int_2^y \frac{du}{\log u} \right| = O\left(x(\log x)^{-A}\right).$$

This led to the striking bound

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} \leq \left(2 + \sqrt{3}\right)/8 = 0.46650\ldots .$$

This was later lowered first by Huxley by the use of more sophisticated kernels [69, 70] and then by Maier [80] who showed how his mechanism for detecting greater oscillations in the distribution of primes could be inserted into the framework of the method. These developments via the large sieve stimulated an enormous amount of work in the area in the '60s and '70s.

Returning to the large sieve inequality, Gallagher [34] noticed that the simple formula

$$F\left(\frac{a}{q}\right) = F(\alpha) + \int_{\alpha}^{a/q} F'(\beta)d\beta$$

can be used to bound

$$S\left(\frac{a}{q}\right)^2$$

in terms of

$$\int_{\frac{a}{q}-\frac{1}{Q^2}}^{\frac{a}{q}+\frac{1}{Q^2}} G(\beta)d\beta$$

with

$$G(\beta) = S(\beta)^2$$

and

$$G(\beta) = S(\beta)S'(\beta)$$

and then by completing to a unit interval, applying Cauchy-Schwarz to the second integral and using Parseval's identity he obtained

$$\lambda \leq \pi N + Q^2.$$

The author remembers being particularly excited by this when he was a post-graduate student because it had the flavour of the Hardy-Littlewood method in it.

Another line of attack on the large sieve inequality is via duality. In general, given a sequence of R real numbers x_r for which $\min_{k \in \mathbb{Z}} |x_r - x_s - k| \geq \delta$ whenever $r \neq s$ one would like to be able find the best possible value of $\lambda = \lambda(N, \delta)$ such that for every sequence of complex numbers a_n one has

$$\sum_{r=1}^{R} \left| \sum_{n=1}^{N} a_n e(x_r n) \right|^2 \leq \lambda \sum_{n \leq N} |a_n|^2.$$

By duality this is equivalent to showing that for every sequence of complex numbers b_r one has

$$\sum_{n=1}^{N} \left| \sum_{r=1}^{R} b_r e(x_r n) \right|^2 \leq \lambda \sum_{r=1}^{R} |b_r|^2.$$

Now if one multiplies out the sums on the left and brings the sum over n inside one finds that the general term is a geometric progression which one can sum. The diagonal terms contribute

$$N \sum_{r=1}^{R} |b_r|^2$$

and the non-diagonal terms contribute two expressions of the kind

$$\sum_{\substack{r=1 \\ r \neq s}}^{R} \sum_{s=1}^{R} \frac{c_r \bar{c}_s}{2i \sin \pi (x_r - x_s)}$$

where $|c_r| = |b_r|$. Now this double sum is vaguely reminiscent of Hilbert's inequality

$$\left| \sum_{\substack{r \in \mathbb{Z} \\ r \neq s}} \sum_{s \in \mathbb{Z}} \frac{c_r \bar{c}_s}{r - s} \right| \leq \pi \sum_r |c_r|^2.$$

Obviously the first place to check out the proofs of this, of course, is the book everyone knows as 'Inequalities' [54]. Hardy, Littlewood and Pólya give Schur's proof of this inequality and following a suggestion of Selberg, Montgomery and the author [83] were able to show that one can take

$$\lambda(N, \delta) = N + \delta^{-1}.$$

Four years later — in 1977 — Paul Cohen pointed out a wrinkle which achieves the best possible bound

$$\lambda(N, \delta) = N - 1 + \delta^{-1}.$$

One spin off from this was that the same method also establishes a version of this for $\mathbb{R}$ rather than the torus $\mathbb{R}/\mathbb{Z}$. Thus if for each n one has $\min_{m \neq n} |x_m - x_n| \geq \delta_n > 0$, then one can show that there is a constant C such that

$$\left| \sum_{m=1}^{N} \sum_{\substack{n=1 \\ n \neq m}}^{N} \frac{a_m \bar{a}_n}{x_m - x_n} \right| < C \sum_{n=1}^{N} |a_n|^2 \delta_n^{-1}.$$

This has applications to mean values of Dirichlet polynomials. It gives

$$\int_0^T \left| \sum_{n=1}^{N} a_n n^{-it} \right|^2 dt = \sum_{n=1}^{N} |a_n|^2 (T + O(n))$$

and the presence of the n in the O-term rather than an N which was all that had been available earlier, can be very useful. In particular, by using only the simple approximation

$$\zeta\left(\frac{1}{2}+it\right) = \sum_{n\leq N} n^{-\frac{1}{2}-it} + O\left(\frac{N^{\frac{1}{2}}}{1+|t|}\right)$$

valid for $|t| \leq N$, instead of the approximate functional equation, Montgomery and the author [85] were able to give a simple proof of Hardy and Littlewood's [41] estimate

$$\int_{-T}^{T}\left|\zeta\left(\frac{1}{2}+it\right)\right|^2 dt = 2T\log T + O(T).$$

At about the same time Selberg [104, §§20, 21] discovered a more direct approach to the large sieve inequality, based on constructing optimal, or close to optimal, trigono-metrical polynomials which approximate the characteristic functions of intervals. Again this is something which has wide application.

Perhaps the most striking development to come out of the large sieve was Bombieri's theorem [5] that

$$\sum_{q\leq x^{1/2}(\log x)^{-B(A)}} \max_{(a,q)=1} \sup_{y\leq x} \left| \sum_{\substack{p\leq y \\ p\equiv a \pmod q}} 1 - \frac{1}{\phi(q)}\int_2^y \frac{du}{\log u} \right| = O\left(x(\log x)^{-A}\right).$$

In many situations this can be used in place of GRH. For example, the asymptotic formula for the number of solutions of

$$n = p + x^2 + y^2,$$

which had been predicted by Hardy and Littlewood by suppressing the minor arcs, and then established by the difficult dispersion method of Linnik [77], was later given a relatively straightforward proof by Elliott and Halberstam [27] in which Bombieri's theorem is combined with a method of Hooley [64]. Also, Bombieri's theorem and a similar result on the distribution of products of primes was an important ingredient in Chen's theorem [10] that every large even number $2n$ satisfies

$$2n = p + P_2$$

where P_2 denotes a number having at most two prime factors.

We now have relatively simple proofs of Bombieri's theorem. In fact we now have a general method which enables us to treat certain sums over primes in a fairly unified way. Thus the same approach will also give an estimate for

$$\sum_{p\leq X}(\log p)e(\alpha p)$$

suitable for use on the minor arcs when the Hardy-Littlewood-Vinogradov method is applied to the ternary Goldbach problem. This approach is based on the following simple identity, [112, 113]. Let

$$\Lambda(n) = \log p$$

when n is of the form p^k and be 0 otherwise.

$$\sum_{n \leq X} \Lambda(n)g(n) = S_1 - S_2 - S_3 + S_4,$$

where

$$S_1 = \sum_{m \leq U} \mu(m) \sum_{n \leq X/m} \log n\, g(mn),$$

$$S_2 = \sum_{m \leq UV} b_m \sum_{n \leq X/m} g(mn),$$

$$S_3 = \sum_{m > U} \sum_{V < n \leq X/m} c_m \Lambda(n)e(\alpha mn),$$

$$S_4 = \sum_{n \leq V} \Lambda(n)g(n),$$

$$b_m = \sum_{r \leq U} \sum_{\substack{s \leq V \\ rs = m}} \mu(r)\Lambda(s),$$

$$c_m = \sum_{\substack{r \leq U \\ r | m}} \mu(r).$$

This and a large family of similar identities have had quite wide application in analytic number theory. The above may look complicated, but it is immediate from the trivial identity

$$-\frac{\zeta'}{\zeta}(s) = -G(s)\zeta'(s) - F(s)G(s)\zeta(s)$$

$$- (G(s)\zeta(s) - 1)\left(-\frac{\zeta'}{\zeta}(s) - F(s)\right) + F(s)$$

This memoir has only begun to scratch the surface of the vast body of applications of the Hardy-Littlewood method. There is a very considerable series of applications to general forms, by Birch [3], Davenport [16], Heath-Brown [59, 62], Hooley [65–67], Schmidt [98–101] and others, and likewise to systems of forms. Another class of problems is concerned with mixed exponents. For example it can be shown that when

the pair k, l is 3, 3 [17], 3, 4 [94] or 3, 5 [114], or 2, l [18] with l arbitrary, then almost every natural number can be written in the form

$$x^2 + y^k + z^l$$

provided that the appropriate local condition is satisfied and that for every other choice of exponents with $2 \le k \le l$ there is a set of positive density which is not represented.

The method has also proved useful in elucidating the general distribution of primes in arithmetical progressions. Results obtained by the Hardy-Littlewood-Vinogradov method have been used by Montgomery [82] to show that when $Q \le x$

$$\sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \log p - \frac{x}{\phi(q)} \right)^2 = Qx \log Q + O\left(Qx + x^2 (\log x)^{-A}\right)$$

and on GRH Goldston and Vaughan [35] have shown that

$$\sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \log p - \frac{x}{\phi(q)} \right)^2$$

$$= Qx \log Q - cQx + O\left(Q^2 (x/Q)^{\frac{1}{4}+\varepsilon} + x^{\frac{3}{2}} (\log x)^{\frac{5}{2}} (\log \log x)^2 \right).$$

Recently the Hardy-Littlewood method has been used to obtain results of this kind regarding the distribution of general sequences into arithmetical progressions [118].

A very ingenious adaptation of the Hardy-Littlewood method was made by Roth [95, 96] in order to show that any subset $\mathscr{A}$ of $[1, n] \cap \mathbb{Z}$ which has no three members in arithmetic progression satisfies card $\mathscr{A} = o(n)$. Later Szemerédi [107] showed by a different method that the conclusion still held even when the hypothesis was weakened to $\mathscr{A}$ having no k members in arithmetic progression. Then Furstenberg [33] gave another proof of Sezemeredi's theorem based on ergodic methods, and some of the other applications of his methods have the flavour of a variant of the Hardy-Littlewood method.

Davenport and Heilbronn [19] introduced an interesting variant of the method which showed that if $\lambda_1, \ldots, \lambda_5$ are not all in rational ratio and not all the same sign, then for each positive number ε there are integers $x_1, \ldots, x_5$, not all zero, such that

$$\left| \lambda_1 x_1^2 + \cdots + \lambda_5 x_5^2 \right| < \varepsilon.$$

Again there has been a good deal of activity attacking more general situations, and achieving more precise estimates. For example Vaughan [111] was able to show that

there are infinitely many solutions in primes p_1, p_2, p_3 to the inequality

$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3| = O(\max(p_i)^{-1/10}(\log \max(p_i))^{20}.$$

Baker and Harman [1], and [58] have taken this further.

Another area of interest has been in developing the method for use in algebraic number fields. Notable moves in this direction have been made by Siegel [105, 106], Rademacher [88], Birch [2], Davidson [20–22]. There is also an increasing interest in applying the method to other rings, for example the ring of polynomials over finite fields, for which see Effinger and Hayes [23].

There has been a very striking recent development by Bombieri and Iwaniec [8, 9] the main objective of which is to obtain non-trivial estimates for exponential sums of the kind

$$\sum_{M+1<n\leq M+N} e(\phi(n))$$

where ϕ is a real valued function of a real variable satisfying certain smoothness conditions. There are famous applications of such estimates to the error term in the Dirichlet divisor problem, to Gauss's problem of counting the number of lattice points in a large circle centered on the origin, and of the order of magnitude of the zeta function on the $\frac{1}{2}$ line (this latter problem is related to the Lindelöf Hypothesis). In their arguments there is a clear division of cases according as to how close the second derivative of ϕ at a particular point is to a rational number with a relatively small denominator. If it is close to such a rational number then there are quite precise estimates available. Otherwise, alternative procedures are required. The division smacks of a division into major and minor arcs. Huxley has taken the methods a good deal further, and as he says [71, p. 470] 'The Hardy-Littlewood method is one of the great themes of number theory this century'. Moreover it seems to be gaining momentum rather than losing it. By 1981 the number of research papers which made some use of the method was almost exactly 400. In the intervening sixteen years that number has more than doubled. It is hard to know how number theory would have developed without Hardy's influence, but it certainly would have done so rather differently. Hardy's legacy is very clearly a lasting one and an immensely rich one.

References

[1] R. C. Baker and G. Harman, 'Diophantine approximation by prime numbers', *J. London Math. Soc.* **25** (1982), 201–215.

[2] B. J. Birch, 'Waring's problem in algebraic number fields', *Proc. Cam. Phil. Soc.* **57** (1961), 449–459.

[3] ———, 'Forms in many variables', *Proc. Royal Soc. London Ser. A* **265** (1962), 245–263.

[4] K. D. Boklan, 'The asymptotic formula in Waring's problem', *Mathematika* **41** (1994), 147–161.

[5] E. Bombieri, 'On the large sieve', *Mathematika* **12** (1965), 201–225.

[6] E. Bombieri and H. Davenport, 'Small differences between prime numbers', *Proc. Royal Soc. London Ser. A* **293** (1966), 1–18.

[7] ———, 'On the large sieve method', in: *Abh. aus Zahlentheorie und Analysis Zur Erinnerung an Edmund Landau* (eut. Verlag Wiss., Berlin, 1968) pp. 11–22.

[8] E. Bombieri and H. Iwaniec, 'On the order of $\zeta(1/2 + it)$', *Ann. Scuola Norm. Pisa Cl. Sci.* **13** (1986), 449–472.

[9] ———, 'Some mean value theorems for exponential sums', *Ann. Scuola Norm. Pisa Cl. Sci.* **13** (1986), 473–486.

[10] J.-R. Chen, 'On the representation of a large even integer as the sum of a prime and the product of at most two primes', *Kexue Tongbao* **17** (1966), 385–386 Foreign Lang. Ed.

[11] N. G. Chudakov, 'On the Goldbach problem', *Comptes Rendus Acad. Sci. URSS* **17** (1937), 335–338.

[12] J. B. Conrey, 'Zeros of derivatives of Riemann's ξ-function on the critical line', *J. Number Theory* **16** (1983), 48–74.

[13] J. G. van der Corput, 'Sur l'hypothèse de Goldbach', *Proc. Akad. Wet. Amsterdam* **41** (1938), 76–80.

[14] H. Davenport, 'On Waring's problem for fourth powers', *Ann. of Math.* **40** (1939), 189–198.

[15] ———, 'On Waring's problem for fifth and sixth powers', *Amer. J. Math.* **64** (1942), 199–207.

[16] ———, 'Cubic forms in sixteen variables', *Proc. Royal Soc. London A* **272** (1963), 285–303.

[17] H. Davenport and H. Heilbronn, 'On Waring's problem: two cubes and one square', *Proc. London Math. Soc.* **43** (1937), 73–104.

[18] ———, 'Note on a result in the additive theory of numbers', *Proc. London Math. Soc.* **43** (1937), 142–151.

[19] ———, 'On indefinite quadratic forms in five variables', *J. London Math. Soc.* **21** (1946), 185–193.

[20] M. Davidson, 'On Waring's problem in number fields', *J. London Math. Soc.* (to appear).

[21] ———, 'On Siegel's conjecture in waring's problem' (to appear).

[22] ———, 'Sums of k-th powers in number fields', *Mathematika* (to appear).

[23] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs (Clarendon Press, Oxford, 1991).

[24] P. D. T. A. Elliott, *Probabilistic number theory: mean value theorems*, Grundlehren der Math. Wiss. 239 (Springer-Verlag, New York, Berlin, Heidelberg, 1979).

[25] ———, *Probabilistic number theory: central limit theorems*, Grundlehren der Math. Wiss. 240 (Springer-Verlag, New York, Berlin, Heidelberg, 1979).

[26] ———, *Duality in analytic number theory* (Cambridge University Press, Cambridge, 1997).

[27] P. D. T. A. Elliott and H. Halberstam, 'Some applications of Bombieri's theorem', *Mathematika* **13** (1966), 196–203.

[28] P. Erdős, 'The difference of consecutive primes', *Duke Math. J.* **6** (1940), 438–441.

[29] P. Erdős and M. Kac, 'On the Gaussian law of errors in the theory of additive functions', *Proc. Nat. Acad. Sci. USA* **25** (1939), 206–207.

[30] ———, 'On the Gaussian law of errors in the theory of additive number theoretic functions', *Amer. J. Math.* **62** (1940), 738–742.

[31] T. Estermann, 'On Goldbach's problem: Proof that almost all even positive integers are sums of two primes', *Proc. London Math. Soc.* **44** (1938), 307–314.

[32] K. B. Ford, 'New estimates for mean values of Weyl sums', in: *Internat. Math. Res. Notices* (1995) pp. 155–171.

[33] H. Furstenberg, 'Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions', *J. d'Analyse Math.* **31** (1977), 204–256.

[34] P. X. Gallagher, 'The large sieve', *Mathematika* **14** (1966), 14–20.

[35] D. A. Goldston and R. C. Vaughan, 'On the Montgomery–Hooley asymptotic formula', in: *Sieve Methods, Exponential sums and their Applications in Number Theory* (eds. G. R. H. Greaves, G. Harman and M. N. Huxley) (Cambridge University Press, Cambridge, 1996).

[36] G. H. Hardy, *A Course of Pure Mathematics* (Cambridge University Press, Cambridge, 1908).

[37] ———, 'Sur les zéros de la fonction $\zeta(s)$ de Riemann', *Comptes Rendus Acad. Sci. Paris Sér. A* **158** (1914), 1012–1014.

[38] ———, 'Goldbach's theorem', *Math. Tid.* **B** (1922), 1–16.

[39] ———, *A Mathematician's Apology* (Cambridge University Press, Cambridge, 1940).

[40] ———, *Ramanujan. Twelve lectures on subjects suggested by his life and work* (Cambridge University Press, Cambridge, 1940).

[41] G. H. Hardy and J. E. Littlewood, 'Contributions to the theory of the Riemann zeta–function and the theory of the distribution of primes', *Acta Mathematica* **41** (1918), 119–196.

[42] ———, 'A new solution of Waring's problem', *Quart. J. Math. Oxford* **48** (1919), 272–293.

[43] ———, 'Some problems of "Partitio Numerorum". I A new solution of Waring's problem', *Göttingen Nachrichten* (1920), 33–54.

[44] ———, 'Some problems of "Partitio Numerorum". II Proof that every large number is the sum of at most 21 biquadrates', *Math. Z.* **9** (1921), 14–27.

[45] ———, 'The zeros of Riemann's zeta–function on the critical line', *Math. Z.* **10** (1921), 283–317.

[46] ———, 'The approximate functional equation in the theory of the zeta function, with applications to the divisor problems of Dirichlet and Piltz', *Proc. London Math. Soc.* **21** (1922), 39–74.

[47] ———, 'Some problems of "Partitio Numerorum". IV The singular series in Waring's problem', *Math. Z.* **12** (1922), 161–188.

[48] ———, 'On Lindelöf's hypothesis concerning the Riemann zeta–function', *Proc. Roy. Soc. A* **103** (1923), 403–412.

[49] ———, 'Some problems of "Partitio Numerorum". III On the expression of a number as a sum primes', *Acta Math.* **44** (1923), 1–70.

[50] ———, 'Some problems of "Partitio Numerorum". V A further contribution to the study of Goldbach's problem', *Proc. London Math. Soc.* **22** (1923), 46–56.

[51] ———, 'Some problems of "Partitio Numerorum". VI Further researches in Waring's problem', *Math. Z.* **23** (1925), 1–37.

[52] ———, 'Some problems of "Partitio Numerorum". VIII The number $\gamma(k)$ in Waring's problem', *Proc. London Math. Soc.* **28** (1928), 518–541.

[53] ———, 'The approximate functional equation for $\zeta(s)$ and $\zeta(s^2)$', *Proc. London Math. Soc.* **29** (1929), 81–97.

[54] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities*, second edition (Cambridge University Press, Cambridge, 1959).

[55] G. H. Hardy and S. Ramanujan, 'Asymptotic formulae in combinatory analysis', *Proc. London Math. Soc.* **17** (1918), 75–115.

[56] ———, 'The normal number of prime factors of a number n', *Quart. J. Math. Oxford* **48** (1920), 76–92.

[57] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1938).

[58] G. Harman, 'Diophantine approximation by prime numbers', *J. London Math. Soc.* **44** (1991), 218–226.

[59] D. R. Heath-Brown, 'Cubic forms in ten variables', *Proc. London Math. Soc.* **47** (1983), 225–257.

[60] ———, 'Weyl's inequality, Hua's inequality, and Waring's problem', *J. London Math. Soc.* **23**

(1988), 396–414.

[61] ——, 'Weyl's inequality, Hua's inequality', in: *Number Theory (Ulm, 1987), Lecture Notes in Math. 1380* (Springer-Verlag, Berlin, 1989) pp. 67–92.

[62] ——, 'The density of zeros of forms for which weak approximation fails', *Math. Comp.* **59** (1992), 613–623.

[63] D. Hilbert, 'Beweis für Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl unter Potenzen Waringsche Problem', *Math. Annalen* **67** (1909), 281–300; *Nachrichten von der Königlichen Gesellchaft der Wissenschaften zu Göttingen mathematischphysikalische Klasse aus den Jahre 1909, pp. 17–36;*.

[64] C. Hooley, 'On the representation of a number as the sum of two squares and a prime', *Acta Math.* **97** (1957), 189–210.

[65] ——, 'On nonary cubic forms. I', *J. reine angew. Math.* **386** (1988), 32–98.

[66] ——, 'On nonary cubic forms. II', *J. reine angew. Math.* **415** (1991), 95–165.

[67] ——, 'On nonary cubic forms. III', *J. reine angew. Math.* **456** (1994), 53–63.

[68] L.-K. Hua, 'On Waring's problem', *Quart. J. Math. Oxford* **9** (1938), 199–202.

[69] M. N. Huxley, 'Small differences between consecutive primes, I', *Mathematika* **20** (1973), 229–232.

[70] ——, 'Small differences between consecutive primes, II', *Mathematika* **24** (1977), 142–152.

[71] ——, *Area, Lattice Points, and Exponential Sums*, London Math. Soc. Monographs, New series 13 (Clarendon Press, Oxford, 1996).

[72] J. Kubilius, 'Probabilistic methods in the theory of numbers', *Uspeki Mat. Nauk* **11** (1956), 31–66 *Americar Math. Soc. Transl.* **19** (1962) pp. 47–85.

[73] N. Levinson, 'More than one third of the zeros of Riemann's zeta–function are on $\sigma = \frac{1}{2}$', *Adv. Math.* **13** (1974), 383–436.

[74] ——, 'A simplification of the proof that $N_0(T) > \frac{1}{3} N(T)$ for Riemann's zeta–function', *Adv. Math.* **18** (1975), 239–242.

[75] ——, 'Deduction of semi-optimal mollifier for obtaining lower bounds for $N_0(T)$ for Riemann's zeta–function', *Proc. Nat. Acad. Sci. USA* **72** (1975), 294–297.

[76] Ju. V. Linnik, 'The large sieve', *Dokl. Akad. Nauk SSSR* **30** (1941), 292–294.

[77] ——, *The dispersion method in binary additive problems*, Transl. by S. Schuur (Amer. Math. Soc., Providence, 1963).

[78] S.-T. Lou, 'A lower bound for the number of zeros of Riemann's zeta–function on $\sigma = \frac{1}{2}$', in: *Recent Progress in Analytic Number Theory. Vol. I* (Academic Press, London, 1981) pp. 319–324.

[79] K. Mahler, 'On the fractional parts of the powers of a rational number II', *Mathematika* **4** (1957), 122–124.

[80] H. Maier, 'Small differences between prime numbers', *Mich. Math. J.* **35** (1988), 323–344.

[81] H. L. Montgomery, 'A note on the large sieve', *J. London Math. Soc.* **43** (1968), 93–98.

[82] ——, 'Primes in arithmetic progressions', *Mich. Math. J.* **17** (1970), 33–39.

[83] H. L. Montgomery and R. C. Vaughan, 'The large sieve', *Mathematika* **20** (1973), 119–13.

[84] ——, 'Error terms in additive prime number theory', *Quart. J. Math. Oxford* **24** (1973), 207–216.

[85] ——, 'Hilbert's inequality', *J. London Math. Soc.* **8** (1974), 73–82.

[86] ——, 'The exceptional set in Goldbach's problem', *Acta Arithmetica* **27** (1975), 353–370.

[87] H. Rademacher, 'On the partition function', *London Math. Soc* **43** (1937), 241–254.

[88] ——, 'Additive algebraic number theory', *Proc. Intern. Congr. Math.* **1** (1950), 356–362.

[89] S. Ramanujan, 'Highly composite numbers', *Proc. London Math. Soc.* **14** (1915), 347–409.

[90] R. A. Rankin, 'The difference between consecutive primes', *J. London Math. Soc.* **13** (1938), 242–247.

[91] ——, 'The difference between consecutive primes, II', *Proc. Cam. Phil. Soc.* **36** (1940), 255–

266.

[92] A. Rényi, 'On the large sieve of Ju. V. Linnik', *Compositio Math.* **8** (1950), 68–75.

[93] G. Ricci, 'Recherches sur l'allure de la suite $\frac{p_{n+1}-p_n}{\log p_n}$', in: *Colloque sur le Théorie des Nombres Bruxelles 1955* (Georges Thone, Liege; Masson and Cie, Paris, 1956) pp. 93–106.

[94] K. F. Roth, 'A problem in additive number theory', *Proc. London Math. Soc.* **53** (1951), 381–395.

[95] ——, 'On certain sets of integers I', *J. London Math. Soc.* **28** (1953), 104–109.

[96] ——, 'On certain sets of integers II', *J. London Math. Soc.* **29** (1954), 2–26.

[97] ——, 'On the large sieves of Linnik and Renyi', *Mathematika* **12** (1965), 1–9.

[98] W. M. Schmidt, 'Small zeros of additive forms in many variables I', *Trans. Amer. Math. Soc.* **248** (1979), 121–133.

[99] ——, 'Small zeros of additive forms in many variables II', *Acta Math.* **143** (1979), 219–232.

[100] ——, 'Diophantine inequalities for forms of odd degrees', *Advances in Math.* **38** (1980), 128–151.

[101] ——, 'The density of integer points on homogeneous varieties', *Acta Math.* **154** (1985), 243–296.

[102] A. Selberg, 'On the zeros of Riemann's zeta-function on the critical line', *Skr. Norske Vid. Akad. Oslo* **10** (1942), ????

[103] ——, 'Reflections around the Ramanujan centenary', in: *Atle Selberg Collected Papers, Vol. I* (Springer-Verlag, Berlin Heidelberg, 1989) pp. 695–706.

[104] ——, 'Lectures on sieves', in: *Atle Selberg Collected Papers, Vol. II* (Springer-Verlag, Berlin Heidelberg, 1991) pp. 65–247.

[105] C. L. Siegel, 'Generalization of Waring's problem to algebraic number fields', *Am. J. Math.* **66** (1944), 122–136.

[106] ——, 'Sums of mth powers of algebraic integers', *Ann. Math.* **246** (1945), 313–339.

[107] E. Szemerédi, 'On sets of integers containing no k elements in arithmetic progression', *Acta Arithmetica* **27** (1975), 199–245.

[108] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics: 46 (Cambridge University Press, Cambridge, 1995).

[109] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function* (Oxford University Press, Oxford, 1951).

[110] P. Turán, 'On a theorem of Hardy and Ramanujan', *J. London Math. Soc.* **9** (1934), 274–276.

[111] R. C. Vaughan, 'Diophantine approximation by prime numbers I, II', *Proc. London Math. Soc.* **28** (1974), 373–384; 385–401.

[112] ——, 'Sommes trigonométriques sur les nombres premiers', *C. R. Acad. Sci. Paris Sér. A* **258** (1977), 981–983.

[113] ——, 'An elementary method in prime number theory', *Acta Arithmetica* **37** (1980), 111–115.

[114] ——, 'A ternary additive problem', *Proc. London Math. Soc.* **41** (1980), 516–532.

[115] ——, 'On Waring's problem for cubes', *J. reine angew. Math.* **365** (1986), 122–170.

[116] ——, 'On Waring's problem for smaller exponents. II', *Mathematika* **33** (1986), 6–22.

[117] ——, 'A new iterative method in Waring's problem', *Acta Math.* **162** (1989), 1–71.

[118] ——, 'On a variance associated with the distribution of general sequences in arithmetic progressions I, II', *Phil. Trans. Royal Soc. London A* **356** (1998), 781–791.

[119] R. C. Vaughan and T. D. Wooley, 'Further improvements in Waring's problem. III: Eighth powers', *Phil. Trans. Royal Soc. London A* **354** (1993), 385–396.

[120] ——, 'Further improvements in Waring's problem, II: Sixth powers', *Duke Math. J.* **?** (1994), 683–710.

[121] ——, 'Further improvements in Waring's problem', *Acta Math.* **174** (1995), 147–240.

[122] I. M. Vinogradov, 'Some theorems concerning the theory of primes', *Recueil Math.* **44** (1937), 179–195.

[123] ——, 'On an upper bound for $G(n)$', *Izv. Akad. Nauk SSSR* **23** (1959), 637–642.

[124] E. Waring, *Meditationes Algebraicæ*, English translation of the third edition, 1782 (American Math. Soc., Providence, 1991).

[125] H. Weyl, 'Über die Geichverteilung von Zahlen mod Eins', *Math. Ann.* **77** (1916), 313–352.

[126] T. D. Wooley, 'Large improvements in Waring's problem', *Ann. Math.* **162** (1992), 1–71.

[127] ——, 'On Vinogradov's mean value theorem', *Mathematika* **39** (1993), 379–399.

Address From 1st January 1999:
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
Current address:
Department of Mathematics
Huxley Building
Imperial College
180 Queen's Gate
London, SW7 2BZ