

## SOME APPLICATIONS OF BOMBIERI'S THEOREM

P. D. T. A. ELLIOTT *and* H. HALBERSTAM

A famous conjecture of Hardy and Littlewood [4] stated that all sufficiently large integers  $n$  could be represented in the form

$$n = p + x^2 + y^2, \quad (1)$$

where  $p$  is a rational prime and  $x, y$  are integers. G. K. Stanley [9] showed that this result held for "almost all" integers  $n$  if one assumed a hypothesis concerning the zeros of  $L$ -functions similar to, though weaker than, the extended Riemann hypothesis.

Important progress was made by Hooley [5], who showed that their conjecture held if one assumed [Hooley, 5; Lemma 1], that if  $\pi(y; k, h)$  denotes the number of primes  $p \equiv h \pmod{k}$  and less than  $y$ ,

$$E(y, k) = \max_{(h, k)=1} \left| \pi(y; k, h) - \frac{\text{li } y}{\phi(k)} \right| = O(y^{\frac{1}{2}} \log 2y).$$

It is well-known that this result is a direct consequence of the extended Riemann hypothesis.

The first proof of (1) free of any hypothesis was given by Linnik [6]. His method, the so-called "Dispersion Method", is very complicated but leads to an asymptotic formula for the number of solutions of (1). Moreover, the same method was applied successfully by him to estimate the sum

$$\sum_{a < p < n} \tau(p - a),$$

where, as usual,  $\tau$  denotes the divisor function.

Recently, G. Rodriques [8] showed that by using Bombieri's theorem [1] on primes in arithmetic progressions, one could give a short proof of the estimate

$$\sum_{a < p < n} \tau(p - a) = bn + O\left(\frac{n \log \log n}{\log n}\right),$$

where  $b = b(a)$  is a positive constant. It is our purpose here to show that, with simple modifications, one can apply Bombieri's theorem to give an alternative proof of (1) by Hooley's powerful method, freed of any hypothesis. At the same time, we investigate to what extent the ideas involved are useful in estimating more general sums of the type

$$S = \sum_{p < n} \sum_{d | (n-p)} f(d), \quad (2)$$

---

H. Halberstam gratefully acknowledges support from the National Science Foundation.

where  $f$  is, for the moment, an arbitrary arithmetic function. (Note that  $f$  has a different meaning in [5].) A similar analysis can be used to discuss sums of the type

$$\sum_{a < p < n} \sum_{d|(p-a)} f(d).$$

Let us consider (2) in detail. For convenience, we shall use  $l$  as an abbreviation for  $\log n$ . We begin in a manner similar to Hooley's by writing the inner sum in (2) as

$$\left( \sum_{\substack{d|(n-p) \\ d \leq n^{1/2} l^{-c}}} + \sum_{\substack{d|(n-p) \\ n^{1/2} l^{-c} < d < n^{1/2} l^c}} + \sum_{\substack{d|(n-p) \\ d \geq n^{1/2} l^c}} \right) f(d)$$

for a positive constant  $C$  to be chosen later, and, in accordance with this subdivision, we write

$$S = S_1 + S_2 + S_3.$$

Now in problems of this type it is natural to expect that  $S_1$  will be as large as any term. Let  $\nu(m)$  denote the number of distinct prime divisors of  $m$  and assume † that

$$f(d) \ll 1. \tag{3}$$

(We use Vinogradov's notation  $\ll$  to indicate an inequality with an unspecified constant factor.) We require first the result of Bombieri mentioned earlier, namely

LEMMA (BOMBIERI [1]). *For any given constant  $c_1 > 0$  there exists a positive constant  $B = B(c_1)$  such that*

$$\sum_{d \leq n^{1/2} l^{-B}} \max_{y \leq n} E(y, d) \ll n l^{-c_1}.$$

Taking  $c_1 = 2$  in the Lemma, and  $C > B(2)$ , we see that

$$\left| S_1 - \sum_{\substack{d \leq n^{1/2} l^{-c} \\ (d, n) = 1}} \frac{f(d)}{\phi(d)} \operatorname{li} n \right| < \sum_{\substack{d \leq n^{1/2} l^{-c} \\ (d, n) = 1}} |f(d)| E(n, d) + \sum_{\substack{d \leq n^{1/2} l^{-c} \\ (d, n) > 1}} |f(d)| \\ \ll n (\log n)^{-2}$$

by (3). Now it is well-known (see, for example, Prachar [7; p. 44, Satz 4.1]) that if  $d < n$ ,  $(h, d) = 1$ , then

$$\pi(n; d, h) \ll \frac{n}{\phi(d) \log(n/d)}$$

---

† Actually, it will be clear from the sequel that the weaker condition  $f(p^\alpha) \ll 1$  suffices for the purpose of estimating effectively the sums  $S_1$  and  $S_2$ . Hence, if also  $f$  is non-negative, the method will be seen to lead, under these alternative conditions on  $f$ , to good lower bounds for  $S$ .

holds uniformly with respect to  $d$  and  $h$ . In [8] this crude upper bound was used to estimate a sum similar to  $S_2$ . If we follow that example and use the fact (Estermann [3]) that

$$\sum_{d < z} \frac{1}{\phi(d)} = \beta \log z + O(1),$$

where  $\beta$  is a positive constant, we obtain

$$S_2 \ll \sum_{n^{1/2} l^{-c} < d < n^{1/2} l^c} \frac{n}{\phi(d) \log n} \ll \frac{n}{\log n} \log \log n.$$

Thus we see easily that, subject to (3),

$$S_1 + S_2 = \frac{n}{\log n} \sum_{\substack{(d, n)=1 \\ d \leq n^{1/2}}} \frac{f(d)}{\phi(d)} + O\left(\frac{n}{\log n} \log \log n\right), \tag{4}$$

where the extension of the range of summation in the sum on the right is justified by the argument used to estimate  $S_2$ .

It is clear that we shall not arrive at an asymptotic formula for  $S$  unless the sum on the right of (4) is large compared with  $\log \log n$ . If, for example,  $f(d)$  is a non-principal character,  $\sum_d f(d)/\phi(d)$  converges and we have only an upper bound for  $S$ . In such cases we have the method of Hooley with which to estimate  $S_2$ . His idea is to write

$$S_2 = \sum_{p < n} \sum_{\substack{d|(n-p) \\ n^{1/2} l^{-c} < d < n^{1/2} l^c}} f(d) = \sum_{p < n} F(n-p),$$

so that by the Cauchy-Schwarz inequality

$$|S_2|^2 \leq \left( \sum_{\substack{p < n \\ F(n-p) \neq 0}} 1 \right) \left( \sum_{p < n} F^2(n-p) \right).$$

The first sum on the right is  $O(n(\log n)^{-1-\delta})$  for some constant  $\delta > 0$ . To estimate the second sum Hooley introduced the integers  $w < n$  having no prime factors  $p \leq \exp\{l/(\log l)^2\}$ ; thus

$$\sum_{p < n} F^2(n-p) \leq \sum_{w < n} F^2(n-w).$$

Now the integers  $w$  are well-distributed (mod  $r$ ) for  $r \leq n^\theta$  where  $\theta$  is any fixed constant satisfying  $0 < \theta < 1$ . We can invert the order of summation to obtain the upper bound  $O_\epsilon(n(\log n)^{-1+\epsilon})$  for any fixed  $\epsilon > 0$ , provided that sums of the type

$$\sum'_{\substack{w=n-s\lambda \\ z_1 \leq w < z_2}} f(s) \tag{5}$$

are of order  $\lambda^{-1}(\log n)^{-1+\epsilon}$ . Here  $\Sigma'$  indicates that  $f(s)$  is "weighted" by a certain function which is essentially 1. Also,  $\lambda$  is an integer satisfying  $\lambda \leq n^\theta$ ,  $0 < \theta < 1$ , and  $z_1, z_2$  satisfy  $z_1 < z_2 \leq n$  (see Hooley [5; 206-208]).

In order to make use of the good distribution of the  $w$  (the only available result) it appears necessary to make  $f(s)$  depend only upon the residue class

of  $s$  modulo  $k$  for some integer  $k < (\log n)^c$ ,  $c > 0$ . Thus, if  $f$  is also completely multiplicative,  $f$  must be a character. If then  $f(s)$  does depend only upon the class of  $s \pmod k$  we see easily that (5) is small when (and only when)

$$\sum_{\substack{s \pmod k \\ (n-s\lambda, k\lambda)=1}} f(s) = 0. \tag{6}$$

Thus, in Hooley's case,  $k=4$ ,  $f(s)=\chi_4(s)$ , a non-principal character modulo 4, and the conditions  $(n-\lambda, 4\lambda)=1$ ,  $(n-3\lambda, 4\lambda)=1$  hold together. Then (6) is true, and

$$S_2 = O\left(n(\log n)^{-1-\delta}\right) \text{ for some } \delta > 0.$$

For more general sums of the type

$$\sum_{p < n} \sum_{n-p=drK} \chi_k(d),$$

where  $dr \equiv H \pmod k$  must hold for certain integers  $K, H$  with  $\chi(H)=1$ , we refer to Bredekhn [2]. He connected such sums with the problem of representing  $n$  as  $p + Q(x, y)$ , where  $Q$  is a certain fixed positive definite quadratic form.

In order to complete the modified Hooley proof we now show that  $S_3$  is, in this case, small. In fact, we have

$$\begin{aligned} S_3 &= \sum_{p < n} \sum_{\substack{d \mid (n-p) \\ d \geq n^{1/2} l^c}} \chi_4(d) \\ &= \sum_{q < n^{1/2} l^{-c}} \sum_{\substack{qd = n-p \\ n^{1/2} l^c \leq d < n/q}} \chi_4(d) \\ &= \sum_{q < n^{1/2} l^{-c}} \left\{ \sum_{\substack{p \equiv n+3q \pmod{4q} \\ p \leq n-qn^{1/2} l^c}} 1 - \sum_{\substack{p \equiv n+q \pmod{4q} \\ p \leq n-qn^{1/2} l^c}} 1 \right\} \\ &\leq 2 \sum_{\substack{q < n^{1/2} l^{-c} \\ (n+q, 4q)=1}} E(n-qn^{1/2} l^c, 4q) + O\left(\sum_{q < n^{1/2} l^{-c}} 1\right) \\ &\ll n(\log n)^{-2}, \end{aligned}$$

provided  $C$  is sufficiently large, by the Lemma. Thus we have proof of the following result : †

**THEOREM 1 (HOOLEY-LINNIK).** *The number of representations of  $n$  as  $p + x^2 + y^2$  is*

$$\frac{\pi n}{\log n} \prod_{p > 2} \left(1 + \frac{\chi_4(p)}{p(p-1)}\right) \prod_{\substack{p \mid n \\ p \equiv 1 \pmod{4}}} \frac{(p-1)^2}{p^2-p+1} \prod_{\substack{p \mid n \\ p \equiv 3 \pmod{4}}} \frac{p^2-1}{p^2-p-1} + O\left(\frac{n}{(\log n)^{1+\delta}}\right)$$

as  $n \rightarrow \infty$ .

---

† In their memoir [4], Hardy and Littlewood actually conjectured the asymptotic formula of Theorem 1 (without the error term).

For the best value of  $\delta$  to date, the estimate of which depends essentially upon improving Hooley's estimate for

$$\sum_{\substack{p < n \\ F(n-p) \neq 0}} 1,$$

we refer to Bredekhn [2], who obtains  $\delta > 0.0425$ .

Similarly, a modified simple proof can be given for the infinitude of primes of the form  $x^2 + y^2 + a$ , with  $a$  a fixed integer.

Let us now return to the estimation of the sum (2) when

$$\sum_{\substack{d \leq n^{1/2} \\ (d, n) = 1}} \frac{f(d)}{\phi(d)}$$

is large. Here, in view of (4), it remains to consider the sum

$$S_3 = \sum_{q \leq n^{1/2} l^{-c}} \sum_{\substack{qd = n - p \\ n^{1/2} l^c \leq d < n/q}} f(d),$$

and we distinguish two possible cases that we can handle. Firstly, it may be possible to relate  $S_3$  to  $S_1$ , as is the case when  $f(d) = 1$ . Here  $S_3 = S_1$  and we conclude that

$$\sum_{p < n} \tau(n-p) = 2 \frac{n}{\log n} \sum_{\substack{d \leq n^{1/2} \\ (d, n) = 1}} \frac{1}{\phi(d)} + O\left(\frac{n}{\log n} \log \log n\right).$$

By a well-known estimate (see, for example, Estermann [3]) we obtain the following result, first proved conditionally by Walfisz [10]:

**THEOREM 2 (LINNIK-BREDEKHIN).** *If  $\zeta$  denotes, as usual, Riemann's zeta-function, we have, as  $n \rightarrow \infty$ ,*

$$\sum_{p < n} \tau(n-p) = \frac{315\zeta(3)}{2\pi^4} \prod_{p|n} \frac{(p-1)^2}{p^2-p+1} n + O\left(\frac{n}{\log n} \log \log n\right).$$

The sum considered here is, of course, in a sense "conjugate" to that studied in [8].

Secondly, we can consider those functions  $f(d)$  which receive their biggest contribution from the small divisors of  $d$ ; this is the case, for example, if  $f(d)$  is of the form

$$f(d) = \sum_{m^2|d} g(m),$$

for the summands  $g(m)$  are, in a sense, weighted in favour of small values of  $m$ . Taking  $g = \mu$ , the Moebius function, we have  $f(d) = \mu^2(d)$ , so that

$$\sum_{d|m} f(d) = 2^{\nu(m)}.$$

Hence we derive the following result.

THEOREM 3. *We have*

$$\sum_{p < n} 2^{v(n-p)} = \phi(n) + O\left(\frac{n}{\log n} (\log \log n)^2\right) \quad (n \rightarrow \infty).$$

*Proof.* From earlier remarks we deduce by (4) (with  $f(d) = \mu^2(d)$ ), that

$$\sum_{p < n} 2^{v(n-p)} = \frac{n}{\log n} \sum_{\substack{d \leq n^{1/2} \\ (d, n) = 1}} \frac{\mu^2(d)}{\phi(d)} + O\left(\frac{n}{\log n} \log \log n\right) + S_3,$$

where

$$\begin{aligned} S_3 &= \sum_{\substack{q < n^{1/2} \\ (q, n) = 1}} \sum_{\substack{qd = n - p \\ n^{1/2} l^C \leq d < n/q}} \mu^2(d) + O(n^\sharp l^{-C}) \\ &= \sum_{\substack{q < n^{1/2} \\ (q, n) = 1}} \sum_{\substack{p \leq n - qn^{1/2} l^C \\ p \equiv n \pmod{q}}} \left\{ \sum_{\substack{s^2 | (n-p)/q \\ s \leq l^{C/3}} \mu(s) + \sum_{\substack{s^2 | (n-p)/q \\ s > l^{C/3}} \mu(s) \right\} + O(n^\sharp l^{-C}) \\ &= S_3' + S_3'' + O(n^\sharp l^{-C}) \end{aligned}$$

say. In each term of the sum  $S_3'$  we have  $s^2 q < n^\sharp l^{-C/3}$ ; accordingly, we apply the Lemma to  $S_3'$ , and, if  $C$  is large enough but fixed, we obtain

$$S_3' = \sum_{\substack{q < n^{1/2} \\ (q, n) = 1}} \sum_{\substack{s \leq l^{C/3} \\ (s, n) = 1}} \frac{\mu(s)}{\phi(s^2 q)} \text{li}(n - qn^\sharp l^C) + O(n(\log n)^{-2}). \quad (7)$$

A straightforward approach suffices to estimate  $S_3''$ . We have

$$\begin{aligned} |S_3''| &\leq \sum_{q \leq n^{1/2}} \sum_{l^{C/3} < s < (n/q)^{1/2}} \sum_{\substack{p \equiv n \pmod{s^2 q} \\ p < n}} 1 \\ &\leq n \sum_{q \leq n^{1/2}} \frac{1}{q} \sum_{s > l^{C/3}} \frac{1}{s^2} \ll n l^{-C/3} \sum_{q \leq n^{1/2}} \frac{1}{q}. \end{aligned}$$

so that

$$|S_3''| < n(\log n)^{-2}. \quad (8)$$

We next consider the multiple sum on the right of (7). This is equal to

$$\sum_{\substack{q < n^{1/2} \\ (q, n) = 1}} \text{li}(n - qn^\sharp l^C) \sum_{\substack{s \leq l^{C/3} \\ (s, n) = 1}} \frac{\mu(s)}{\phi(s^2 q)} = \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{1}{\phi(m)} \sum'_{m = s^2 q} \mu(s) \text{li}(n - qn^\sharp l^C)$$

where  $\Sigma'$  indicates that  $s \leq l^{C/3}$  and  $q < n^\sharp l^{-C}$ . Removing the first of these conditions on the right-hand side introduces an error of order at most

$$\begin{aligned} \text{li } n \sum_{m \leq n^{1/2}} \frac{\log \log m}{m} \sum_{\substack{m = s^2 q \\ s > l^{C/3}}} 1 &\leq n \sum_{q \leq n^{1/2}} \frac{1}{q} \sum_{s > l^{C/3}} \frac{1}{s^2} \\ &< n(\log n)^{-2}, \end{aligned}$$

where we have used Euler's result that  $\phi(m) \gg m(\log \log m)^{-1}$ . We next replace the condition  $q \leq n^{\frac{1}{2}} l^{-c}$  by  $q \leq n^{\frac{1}{2}} l^{-2c}$ , thereby introducing an error of order at most

$$\begin{aligned} \text{li } n \sum_{m \leq n^{1/2}} \frac{1}{\phi(m)} \sum_{\substack{m = s^2 q \\ n^{1/2} l^{-2c} < q \leq n^{1/2} l^{-c}}} 1 &\ll (\text{li } n) \log \log n \sum_{n^{1/2} l^{-2c} < q \leq n^{1/2} l^{-c}} \frac{1}{q} \\ &\ll \frac{n}{\log n} (\log \log n)^2. \end{aligned}$$

Hence, in view of (7) and (8), we have

$$\begin{aligned} S_3 &= \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{1}{\phi(m)} \sum_{\substack{m = s^2 q \\ q \leq n^{1/2} l^{-2c}}} \mu(s) \text{li}(n - qn^{\frac{1}{2}} l^c) + O\left(\frac{n}{\log n} (\log \log n)^2\right) \\ &= \text{li } n \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{1}{\phi(m)} \sum_{\substack{m = s^2 q \\ q \leq n^{1/2} l^{-2c}}} \mu(s) + O\left(\frac{n}{\log n} (\log \log n)^2\right) \\ &\quad + O\left(\frac{n^{\frac{1}{2}} (\log n)^c}{\log n} \log \log n \sum_{m \leq n^{1/2}} \frac{1}{m} \sum_{\substack{m = s^2 q \\ q \leq n^{1/2} l^{-2c}}} q\right) \\ &= \text{li } n \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{1}{\phi(m)} \sum_{m = s^2 q} \mu(s) + O\left(\frac{n}{\log n} (\log \log n)^2\right) \\ &= \frac{n}{\log n} \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{\mu^2(m)}{\phi(m)} + O\left(\frac{n}{\log n} (\log \log n)^2\right). \end{aligned}$$

It follows from this and (4) that

$$S = \frac{2n}{\log n} \sum_{\substack{m \leq n^{1/2} \\ (m, n) = 1}} \frac{\mu^2(m)}{\phi(m)} + O\left(\frac{n}{\log n} (\log \log n)^2\right);$$

by standard methods with Dirichlet series one can prove that

$$\sum_{\substack{m < z \\ (m, n) = 1}} \frac{\mu^2(m)}{\phi(m)} = \frac{\phi(n)}{n} \log z + O\left((\log \log n)^2\right)$$

provided  $n \leq z^5$ , and this completes the proof of the theorem.

In a similar manner we can show that

**THEOREM 4.** *We have*

$$\sum_{a < p < n} 2^{\nu(p-a)} = \frac{\phi(a)}{a} n + O\left(\frac{n}{\log n} (\log \log n)^2\right), \quad (n \rightarrow \infty).$$

It does not appear easy to generalise this result so as to replace 2 by 3.

We are indebted to the referee for his careful scrutiny of an earlier version of this paper.

*References*

1. E. Bombieri, "On the large sieve", *Mathematika*, 12 (1965), 201–225.
2. B. M. Bredekhn, "The dispersion method and binary additive problems", see *Russ. Math. Surveys*, 20 (2), March–April (1965), 85–126.
3. T. Estermann, "On an asymptotic formula due to Titchmarsh", *Journal London Math. Soc.*, 6 (1931), 250–251.
4. G. H. Hardy and J. E. Littlewood, "Some problems of partitio numerorum III. On the expression of a number as a sum of primes", *Acta Math.*, 44 (1922), 1–70.
5. C. Hooley, "On the representation of a number as the sum of two squares and a prime", *Acta Math.*, 97 (1957), 189–210.
6. Yu. V. Linnik, "An asymptotic formula in the Hardy–Littlewood additive problem", *Izv. Akad. Nauk SSSR, Ser. Mat.*, 24 (1960), 629–706.
7. K. Prachar, *Primzahlverteilung* (Springer, Berlin 1957).
8. G. Rodriques, "Sul problema dei divisori di Titchmarsh", *Bollettino Unione Matematica Italiana* (3), 20 (1965), 358–366.
9. G. K. Stanley, "On the representation of numbers as a sum of squares and primes", *Proc. London Math. Soc.* (2), 29 (1928), 122–144.
10. A. Z. Walfisz, "On the theory of prime numbers", *Sobshch. Akad. Nauk Gruzin. SSR*, 14 (1953), 77–83.

University of Nottingham.

University of Michigan.

(Received on the 14th of July, 1966.)