DIOPHANTINE APPROXIMATION

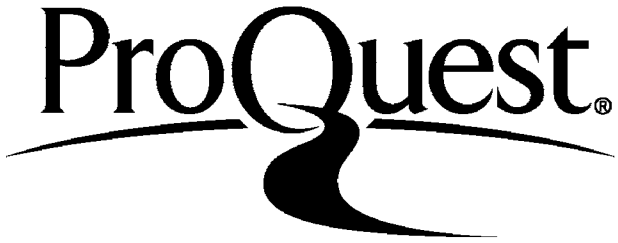
AND

PRIME NUMBERS

by GLYN HARMAN

of ROYAL HOLLOWAY COLLEGE.

For the Ph.D. degree (LONDON).



ABSTRACT.

In the first part of this thesis various problems in diophantine approximation are considered, which generalize well known theorems of Dirichlet and Kronecker. A brief survey is presented in the first chapter, including a discussion on the scope of elementary methods. It is demonstrated here that stronger results are possible by elementary means than have previously been obtained. In the subsequent chapters non-elementary methods are used. Results are proved for fractional parts of quadratic forms in several variables which improve upon previous work. New theorems are demonstrated for the distribution modulo one of "almost all" additive forms in many variables, including the particularly interesting case of a linear form in positive variables. In chapter four new bounds are given for exponential sums over primes, which greatly improve upon the work of I.M. Vinogradov. Some applications to diophantine approximation problems involving primes are given in chapters 4 and 5, the latter chapter also improving upon previous work on the problem of a linear form in three prime variables.

In the second section, topics in multiplicative number theory are discussed. It is shown that almost-primes are very well distributed in almost all very short intervals, improving upon previous work by a considerable factor. Sieve methods are then employed to tackle three other problems. New results are in this way obtained for primes in short intervals, for the distribution of the square roots of primes (modulo one), and for the distribution of αp modulo one for irrational α. This last chapter contains a new method for tackling sums over primes which has other applications.

CONTENTS

NOTATION

We write $\| x \|$ for the distance of x from the nearest integer. We use $\{x\}$ to denote the fractional part of x, that is the distance of x from the next lowest integer if x is not an integer, and zero if x is integral. Sometimes $\{\ \}$ is also used in the standard fashion in the definition of sets. No confusion should arise over these different uses of notation. We write $e(x) = e^{2\pi ix}$. We use the conventional o, O, and $\ll$ notations. Constants implied by these symbols may depend on certain parameters (ε, k, etc.) which are regarded as fixed so far as the question in hand is concerned. Occasionally the dependence of a constant on one of the parameters will be indicated by $\ll_\varepsilon$, etc.

The letter p is reserved for a prime number. Normally P_r represents a number with precisely r prime factors. We use $\Lambda(n)$, the usual von Mangoldt function, defined to be $\log p$ if $n = p^r$, or zero otherwise. We write $\mu(n)$ for the Mobius function, which is zero if n is not square free, and is $(-1)^{\omega(n)}$ otherwise, where $\omega(n)$ is the number of prime factors of n. We write $\pi(x)$ for the number of primes not exceeding x, and

$$\psi(x) = \sum_{n \leq x} \Lambda(n) .$$

In chapters six to ten the letter s is used for a complex variable with $s = \sigma + it$.

PREFACE

The contents of this thesis are based on the research performed by myself at Royal Holloway College 1979-1982. In order to keep the present account as unified as possible, and also to avoid undue length, certain aspects of my research have been omitted (such as my work on irregularities of distribution and the sums of distances between points on an n-dimensional sphere). In the first section of the thesis we shall consider problems in diophantine approximation, including diophantine approximation by prime numbers. This leads naturally on to further questions concerning the distribution of primes, which are considered in section 2. Much of the work in this thesis is already published, or shortly to appear in various papers, references to which are given in the relevant chapters.

I would like to thank London University for awarding me a Postgraduate Studentship, which formed the main financial support for my three postgraduate years at Royal Holloway College. I would like to express my gratitude to Dr. R.C. Baker, firstly for taking me on as a research student, and secondly for his encouragement and advice (although the latter was not always heeded !). Two chapters of the present thesis describe work done with R.C. Baker, and further details of our respective contributions to that work are given in the pertinent places. I would also like to thank Mrs. B. Alderman, Mrs M. Brooker, and Mrs. M. Dixon who typed many of the preprints of my papers, which form the bulk of this thesis. I would also like to thank my mother, Mrs. D.Harman, who typed the references at the back of this thesis.

SECTION ONE

DIOPHANTINE APPROXIMATION

CHAPTER ONE INTRODUCTION

1. In the first part of this thesis we shall be concerned with adaptations of Dirichlet's famous theorem in Diophantine Approximation which may be stated in the following general way :

Given rs real numbers α_{ij} $(i=1,\ldots,r;\ j=1,\ldots,s)$, s positive integers N_j, r positive integers M_i with

$$\prod_{i=1}^{r} M_i \leq \prod_{j=1}^{s} N_j$$

Then there are integers $n_1,\ldots,n_s$, $m_1,\ldots,m_r$ such that

$$\left| \sum_{j=1}^{s} \alpha_{ij} n_j - m_i \right| < M_i^{-1} \qquad (i=1,\ldots,r)$$

and

$$0 < \max_j |n_j| ,$$

while

$$|n_j| \leq N_j \qquad (j=1,\ldots,s).$$

The proof is, of course, a simple application of the box principle. It appears that Hardy and Littlewood [14b] were the first to conjecture what results might be possible if the n_j were replaced by n_j^k for an integer $k \geq 2$. In the 1920's Vinogradov proved the following result :

For all real α, $\varepsilon>0$, and any integer k,

$$\min_{1\leq n\leq N} || \alpha n^k || < N^{-\rho+\varepsilon} \qquad \text{for } N > N(\varepsilon,k).$$

Here $\rho = k(k2^{k-1}+1)^{-1}$ (for example $\rho = 2/5$ for $k=2$).

The proof appears in [22] . Behnke [6] had earlier considered the distribution of the fractional parts of αn^2. The sharpest known result for $k = 2$ is due to Heilbronn [16] and is usually refered to as

Heilbronn's Theorem. He showed that one may take $\rho = \frac{1}{2}$ in this case (Hardy and Littlewood had conjectured $\rho = 1$). The sequence αn^2 has certain properties which make it useful for generating random numbers for Monte Carlo procedures in computing [17]. Danicic showed [10], a little more generally, that one may take $\rho = 2^{1-k}$. For large k better results are available using Vinogradov's methods (e.g. [25] Chapter 5). In particular, R.C. Baker has recently shown [3] that one may take

$$\rho = (\log k)/(4k(\log k + 1)\log(k\log k + 1)).$$

The methods have been extended to cover αn^k replaced by f(n) where f is a polynomial without constant term [25, 13, 20, 4] as well as simultaneous approximation questions [10, 11, 18, 20, 2, 5]. The general idea in the proofs is to convert the problem into a question of estimating exponential sums by using a function which is an approximation to the characteristic function of a small interval while possessing a convenient fourier expansion. We shall utilise this method also. In view of the proof of Dirichlet's theorem it would be nice to have a simple proof of these results, but the only inequality of the above type obtained by elementary means which has appeared in the literature is the rather weak :

$$\min_{1 \leq n \leq N} \| \alpha n^2 \| < \frac{10 \log\log N}{\log N} \quad \text{for } N > e^e.$$

This was shown by R.C. Baker [1] using an ingenious repeated use of the box principle.

It is possible, however, to obtain the exponent ρ given by Vinogradov using only elementary methods. This may be done since Van der Corput and Pisot set out to base the theory of uniform distribution modulo one on elementary considerations alone, and they obtained results for the discrepancy of sequences which are analogous

to the Weyl sum estimates used in those proofs employing Fourier series. They showed [8, 9] :

Let $\eta > 0$ and let $f(x)$ be a polynomial of degree k and leading coefficient α. Suppose

$$| q\alpha - a | < q^{-1} \quad \text{with} \quad (a,q) = 1.$$

Then

$$D_N << N^{\epsilon} (1/q + 1/N + q/N^k)^{2^{1-k}}.$$

Here

$$D_N = \sup_{I \subset [0,1)} \left| \frac{1}{N} \sum_{1}^{N} \chi_I(f(n)) - |I| \right|$$

where $\chi_I(x)$ is the characteristic function of an interval $I \subset [0,1)$ extended to be periodic with period one.

Now put $\lambda = 2^{k-1}\rho$. By Dirichlet's theorem there is a natural number $q \leq N^{k-\lambda}$ and an integer a with

$$| q\alpha - a | < N^{-k+\lambda} \quad \text{and} \quad (a,q) = 1.$$

If $q < N^{\lambda}$ then

$$|| q^k\alpha || < q^{k-1} || q\alpha || < N^{(k-1)\lambda} N^{-k+\lambda} = N^{-\rho}$$

However, for $q \geq N^{\lambda}$ we have

$$D_N << N^{-\rho} + \varepsilon/2$$

and so there is one n with $1 \leq n \leq N$ and having

$$|| n^k\alpha || < N^{-\rho} + \varepsilon$$

assuming N is sufficiently large. This proves Vinogradov's result. Similarly one may prove

For all real α, β and $N > N(\varepsilon)$ we have

$$\min_{1 \leq n \leq N} || \alpha n^2 + \beta n || < N^{-2/7 + \varepsilon}$$

and

Given $\varepsilon > 0$, and a polynomial $f(x)$ of degree k with irrational leading coefficient. Then, for infinitely many n,

$$|| f(n) || < n^{-2^{1-k}} + \varepsilon .$$

One appears to be handicapped when trying to prove the sharpest known results by completely elementary means with the need to consider functions which behave like the characters of the addition group modulo q. It is possible to prove Heilbronn's Theorem without fourier analysis however, by noting that his result is equivalent to :

Let $\varepsilon > 0$, $N > N(\varepsilon)$; suppose a,q are integers satisfying $N < q \leq N^{3/2 - \varepsilon}$, $(a,q) = 1$. Then there are integers n, s with

$$1 \leq n \leq N, \quad |s| \leq \frac{qN^{-\frac{1}{2}} + \varepsilon}{2} , \quad n^2 a \equiv s \pmod{q} . \qquad (2)$$

The result (2) may be established using only Weyl's inequality (see Lemma 2 below) together with the following simple results :

$$\sum_{n=1}^{q} e(\frac{an}{q}) = \begin{cases} 0 & \text{if q does not divide a} \\ q & \text{if q does divide a} \end{cases}$$

$$\sum_{n=1}^{N} e(\alpha n) \ll \min(N, \frac{1}{||\alpha||})$$

The above observation does not seem to have appeared in the literature before.

2. Other extensions of Dirichlet's Theorem.

Vinogradov also demonstrated the following result (see chapter 11 of [25]) :

Let $\varepsilon > 0$, β real be given. Then, for an irrational number α there are infinitely many solutions in primes p of

$$|| \alpha p + \beta || < p^{-1/5 + \varepsilon}.$$

Vinogradov also established results which imply weaker inequalities for p^k with $k \geq 2$ [23,24] . Vinogradov did not exploit fully the strength

3. General Lemmata

We shall state here some basic results which will be needed in the following chapters. The first lemma, in a less general form, was pointed out to the present writer and R.C. Baker by H.L. Montgomery :

LEMMA 1 *Let* L, M *be natural numbers*, β *a real number, and let* $\alpha_1, \ldots, \alpha_M$ *be real numbers such that* $\| \alpha_n - \beta \| \geq L^{-1}$ $(n = 1, \ldots, M)$. *Then we have*

$$\sum_{\ell=1}^{L} \left| \sum_{n=1}^{M} a_n e(\ell\alpha_n) \right| \geq \frac{1}{6} \sum_{n=1}^{M} a_n$$

For any sequence of non-negative real numbers a_n.

Proof Let J be the interval $J = (L^{-1}, 1 - L^{-1})$ with characteristic function $\chi_J(x)$. According to Montgomery [19], p.559, there is a function $b \in L^1(R)$ such that

$$b(x) \geq \chi_J(x), \quad \hat{b}(0) = |J| + L^{-1}$$

and

$$\hat{b}(t) = 0 \quad \text{for} \quad |t| \geq L.$$

Here $\hat{b}(t)$ is the fourier transform of b. By an easy calculation, the function

$$B(x) = \sum_{n} b(x + n)$$

is in $L^1(0,1)$ with fourier series

$$\sum_{|k| \leq L} \hat{b}(k)\, e(kx).$$

Now, for a non zero integer k, this implies that

$$|\hat{b}(k)| \leq \int_0^1 |B(x) - 1|\, dx$$

$$\leq \int_0^1 \{(B(x) - 1) + 2(1 - \chi_J(x))\}\, dx = \hat{b}(0) + 1 - 2|J| = 3L^{-1}.$$

Hence

of his method, however, and in the case k = 1 should have obtained the exponent $\frac{1}{4}$. This result was first demonstrated by R.C. Vaughan [21] using a simpler, though essentially equivalent method. We shall consider problems involving αp^k in Chapter 4. In Chapter 3 we shall also consider a generalization of Vaughan's result to simultaneous approximation for almost all s-tuples. We shall improve Vaughan's result itself in chapter 10.

R.J. Cook [7] proved the following extension of Heilbronn's Theorem :

Let $\varepsilon > 0$ be given; suppose α_1, α_2 are real. Then, for $N > N(\varepsilon)$, there are integers n_1, n_2 with

$$0 \leq n_1,\ n_2 \leq N \quad \text{and} \quad n_1 + n_2 \geq 0$$

having

$$|| \alpha_1 n_1^2 + \alpha_2 n_2^2 || < N^{-1+\varepsilon} .$$

This is near to being best possible as is shown by the following (unpublished) example of R.C. Baker. Let q be squarefree and have all its prime factors congruent to 3 (mod 4). Then, for any a with $(a,q) = 1$ we have

$$\left|\left| \frac{a(n_1^2 + n_2^2)}{q} \right|\right| \geq \frac{1}{q}$$

for $0 \leq n_1,\ n_2 \leq q - 1$, and $n_1 + n_2 > 0$ using Theorem 366 of [15] . Extensions of Heilbronn's Theorem to quadaratic forms are considered in Chapter 2. In Chapter 3 we shall look at generalizations to additive forms in kth powers as well as considering an analogue of Dirichlet's Theorem where the n_j are restricted to be positive integers. In Chapter 5 we shall obtain results for

$$\left| \sum_{j=1}^{s} \lambda_j p_j^{r(j)} + \beta \right| < (\max p_j)^{-\sigma} .$$

Here the p_j are primes, and the r(j) are positive integers.

$$\sum_{n=1}^{M} a_n \leq \sum_{n=1}^{M} a_n B(\alpha_n - \beta) = \sum_{n=1}^{M} a_n \hat{b}(0) + \sum_{\substack{k=-L \\ k\neq 0}}^{L} \hat{b}(k) \sum_{n=1}^{M} a_n e(k(\alpha_n - \beta))$$

$$\leq \sum_{n=1}^{M} a_n \hat{b}(0) + \sum_{0<|k|\leq L} |\hat{b}(k)| \left| \sum_{n=1}^{M} a_n e(k(\alpha_n - \beta)) \right|$$

$$\leq \sum_{n=1}^{M} a_n \hat{b}(0) + \sum_{k=1}^{L} 6L^{-1} \left| \sum_{n=1}^{M} a_n e(k\alpha_n) \right|$$

The result follows since $1 - \hat{b}(0) = L^{-1}$.

The above lemma improves upon Lemma 12 of [25] which gives an infinite fourier series. Lemma 1 is essentially best possible, as has been remarked by H.L. Montgomery (in conversation). This may be seen by considering the example

$$\sum_{\ell=1}^{M-1} \left| \sum_{n=1}^{M} e\left(\frac{\ell n}{M}\right) \right| = 0.$$

LEMMA 2 (Weyl's inequality) Let $g(x)$ be a real valued polynomial of degree k with leading coefficient β. Then, for $\varepsilon > 0$, $R = 2^{k-1}$,

$$\left| \sum_{n=1}^{X} e(g(n)) \right|^R \ll X^{R-k+\varepsilon} \sum_{y=1}^{kX^{k-1}} \min\left(X, \frac{1}{\|\beta y\|}\right)$$

$$\ll X^{R+\varepsilon} \left(1/X + q/X^k + 1/q\right) \qquad (3).$$

Also, for any L, we have

$$\sum_{\ell=1}^{L} \left| \sum_{n=1}^{X} e(\ell g(n)) \right|^R \ll (LX^R)^{1+\varepsilon} \left(1/X + q/(LX^k) + 1/q\right) \qquad (4)$$

Where (3) and (4) hold if $|q\beta - a| < q^{-1}$ with $(q,a) = 1$.

The first version of this result is due to Weyl [26] in his celebrated memoir on the uniform distribution of sequences modulo one. The result, as given in (3) above, was first published by Hardy and Littlewood [14]. For proofs in more recent books see [12] (lemma 1) or [20] (Chapter 10). The last reference also gives estimates for

Weyl sums depending on the second coefficient of $g(x)$. This work has been extended to cover all the coefficients of g by R.C. Baker [4]. Better results are known for large k using Vinogradov's method [25]. Stronger estimates are obtainable when the rational approximation to the leading coefficient is known to be "good". This is demonstrated by the following result of the author's :

LEMMA 3 Given $\delta > 0$, $\varepsilon > 0$, α real, $N > N(\varepsilon, \delta, k)$. Suppose that there are integers q,a with $(q,a)= 1$, $1 \leq q \leq N^{1-\varepsilon}$, $| q\alpha - a | < N^{1-k-\varepsilon}$, and there is a number C with $C \geq \min (N^{1-1/k + \varepsilon}, N^{\frac{3}{4} + \varepsilon})$ with

$$\left| \sum_{n=1}^{N} e(\alpha n^k) \right| > C.$$

Then there is a natural number $r < (N/C)^2 N^{\delta}$ with

$$|| \alpha r^k || < N^{k + \delta} C^{-2k}.$$

The proof will appear in [5]. The result is interesting for it enables one to prove Danicic's result on αn^k with $k \geq 3$ by quite a weak argument. In [5] it is applied to a problem in simultaneous approximation. To prove Danicic's result, let $L = N^{1/2^{k-1} - \varepsilon}$. Then, if the theorem is false, by Lemma 1 we have that

$$\sum_{\ell=1}^{L} \left| \sum_{n=1}^{N} e(\alpha \ell n^k) \right| >> N.$$

Hence, for one ℓ,

$$\left| \sum_{n=1}^{N} e(\alpha \ell n^k) \right| >> NL^{-1}.$$

By Lemma 2 and Dirichlet's Theorem, there is a q with $1 \leq q \leq N^{1-\varepsilon}$ and $|| \ell \alpha q || < N^{1-k-\varepsilon}$. Hence, by Lemma 3, there is an r with

$$|| \ell \alpha r^k || < N^{k + \delta} (NL^{-1})^{-2k}.$$

Thus

$$|| \ell^k r^k \alpha || < N^{-k + \delta} L^{3k-1} < L^{-1}.$$

Also $r\ell < L^3 N^{\delta} < N$. This contradicts the assumption that the theorem is false. The frustrating element in the above proof is that Lemma 2 is neededto obtain a rational approximation "good enough" to enable Lemma 3 to be applied. We are thus unable to improve Danicic's result even though the conclusion we get from Lemma3 is much stronger than is required.

References to Chapter One

1. R.C. Baker, "Recent results on fractional parts of polynomials", Number Theory Carbondale 1979, 10-19, Lecture Notes in Mathematics no. 751, Springer, Berlin 1979.

2. ——— "Fractional parts of several polynomials III," Quart. Journal Math. Oxford (2), 31 (1980), 19-36.

3. ——— "Small fractional parts of the sequence αn^k", Michigan Mathematical Journal, 28 (1981) 223-228.

4. ——— "Weyl sums and diophantine Approximation," J. London Math. Soc. (2), 25(1982), 25-34

5. R.C. Baker and G. Harman, "Small fractional parts of Polynomials", Proceedings of the Colloquium on Number Theory, Budapest 1981, To appear.

6. H. Behnke, "Zur Theorie der diophantische Approximationen I", Abh. Math. Sem. Hamburg 3, 261-318 (1924).

7. R.J. Cook, "On the fractional parts of an additive form," Proc. Camb. Phil. Soc. 72 (1972), 209-212.

8. & 9. J.G. Van der Corput & Ch. Pisot, "Sur la discrepance modulo I & II", Proc. Kon. Ned. Akad. v. Wetensch. Amsterdam, 42 (1939), 476-485 & 554 - 565.

10. I. Danicic, Ph.D. Thesis London 1957

11. ——— , "On the fractional parts of θx^2 and ϕx^2", J. London Math. Soc. 34 (1959), 353-357.

12. H.Davenport, Analytic Methods for diophantine equations and diophantine inequalities, Lecture notes, Univ. of Michigan, 1962.

13. ——— , "On a theorem of Heilbronn", Quart. J. Math. Oxford (2), 18 (1967), 339-344.

14. G.H. Hardy and J.E. Littlewood, "On Partitio Numerorum I", Göttinger Nachrichter, 1920, 33-54.

14b. ———————————— , "Some problems of diophantine approximation", Acta Math. 37 (1914) 155-191.

15. G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford, fifth edition 1979.

16. H. Heilbronn, "On the distribution of the sequence $n^2\theta \pmod 1$", Quart. J. Math. Oxford (1), 19 (1948), 249-256.

17. D.L. Jagerman, "The autocorrelation and joint distribution functions of the sequences $\{(a/m)j^2\}$, $\{(a/m)(j + \tau)^2\}$" Math. Comp. 18 (1964) 211-232.

18. M.C. Liu, "On the fractional parts of θn^k and ϕn^k", Quart. J. Math. Oxford (2), 21 (1970), 481-486.

19. H.L. Montgomery, "The analytic principle of the large sieve", Bull. Amer. Math. Soc. 84 (1978), 547-567.

20. W.M. Schmidt, Small fractional parts of polynomials, American Math. Soc., Providence 1977.

21. R.C. Vaughan, "On the distribution of αp modulo one", Mathematika 24, 48 (1977) 136-141.

22. I.M. Vinogradov, "On the fractional parts of integral polynomials" (Russian), Izv. Akad. Nauk SSSR 20, 585-600.

23. ————————, "A new estimate of a trigonometric sum containing primes", ibid. Ser. Mat. 2 (1938) 1-13.

24. ————————, "On the estimation of a trigonometric sum over primes", ibid. Ser. Mat. 12 (1948) 225-248.

25. ————————, The method of trigonometric sums in the theory of numbers, Wiley Interscience New York, 1954.

26. H. Weyl, "Über die Gleichverteilung von Zahlen mod Eins", Math. Ann. 77, 313-352 (1916).

CHAPTER TWO SMALL FRACTIONAL PARTS OF QUADRATIC FORMS

1. We now consider generalizations of Heilbronn's Theorem of the following form :

For $\varepsilon > 0$, $N > c_1(\varepsilon, s)$ and a quadratic form $Q(x_1, \ldots, x_s)$ there exist integers $n_1, \ldots, n_s$ not all zero, with $|n_1|, \ldots |n_s| \leq N$ and having

$$|| Q(n_1, \ldots, n_s) || < N^{-c_2(s) + \varepsilon} \qquad (1)$$

I. Danicic obtained a result of this type [2] with $c_2(s) = s/(s+1)$. As was remarked in Chapter One, Cook was able to get (1) with $c_2(2) = 1$ provided the quadratic form was additive. More recently A. Schinzel, H.-P. Schlickewei and W.M. Schmidt have shown [7] that $c_2(s)$ may be taken as the maximum of

$$2(1 + h^{-1} + 4/(s - h + 1))^{-1}$$

over odd h with $1 \leq h \leq (s+5)/3$. Taking h asymptotically equal to $s/3$ gives

$$c_2(s) = 2 - (18/s) + O(1/s^2).$$

This result improves upon Danicic's result for $s \geq 7$ and, as is well known, the "limiting" exponent -2 is best possible. To see this we note that

$$|| \sqrt{2}\,(n_1^2 + \ldots\ldots + n_s^2) || > (3sN^2)^{-1}$$

for any N and $0 < \max_i |n_i| \leq N$.

The new idea in [7] is the use of an auxiliary result on quadratic congruences. This method has been refined by R.C. Baker and myself [1] to prove the following result :

THEOREM 1 Let $s \geq 3$ and let $Q(x_1,\dots,x_s)$ be a quadratic form. Then there is a constant $c_4(s)$ such that for every integer $N \geq 2$ there are integers $n_1,\dots,n_s$ with

$$0 < \max(|n_1|,\dots,|n_s|) \leq N , \tag{2}$$

having

$$\| Q(n_1,\dots,n_s) \| < c_4(s)(N/\log N)^{-c_3(s)} \tag{3}$$

Here

$$c_3(s) = \begin{cases} 2s/(s+5) & \text{for odd } s , \\ 2s(s-1)/(s^2+4s-4) & \text{for even } s . \end{cases} \tag{4}$$

Our exponent is the same as Danicic's for $s = 3$, apart from the substitution of a power of $\log N$ for N^{ε}. For $s \geq 4$, our exponent is better than that of [2] or [7], and (4) gives

$$c_3(s) = 2 - (10/s) + O(1/s^2) .$$

In the following proof the idea to use Lemma 1 for additive forms came from R.C. Baker, the extension of the proof to general quadratic forms was made by myself. In section 4 I discuss forms with free variables.

The key to the improvement on [7] is Lemma 1, below. This is a straightforward extension of the congruence result of [7], but enables us to introduce successive minima explicitly. This is more economical; the procedure is analogous to that of Davenport and Ridout [4].

2. Quadratic congruences

LEMMA 1. Let $Q(\underline{x}) = Q(x_1,\dots,x_h)$ be a quadratic form in an odd number h of variables. Let m be a natural number. Let $K_1,\dots,K_h$ be positive reals with

$$K_1 \dots K_h \geq m^{(h+1)/2} . \tag{5}$$

$$|s_i| < m , \qquad (i = 1,\dots,d) \tag{9}$$

$$\Big|\sum_{k=1}^{d} s_k r_{kj} + m z_j\Big| \leq K_j \qquad (j = 1,\dots,h) \tag{10}$$

Put $\underline{\underline{x}} = s_1 \underline{\underline{r}}_1 + \dots + s_d \underline{\underline{r}}_d + m \underline{\underline{z}}$, where $\underline{\underline{z}} = (z_1,\dots,z_h)$. Then clearly (6) holds, and (7) follows from (10) . Since $K_j < m$ we easily see that $(s_1,\dots,s_h) \neq \underline{0}$, say $s_1 \neq 0$. Since m is square free, there is a prime factor p of m with $s_1 \not\equiv 0 \pmod p$. Because $\underline{\underline{r}}_1,\dots,\underline{\underline{r}}_d$ are linearly independent (mod p) , we have $\underline{\underline{x}} \not\equiv 0 \pmod p$. Thus $\underline{\underline{x}} \neq 0$.

3 . Proof of the Theorem. The proof will be by contradiction. Suppose that there are no integers $n_1,\dots,n_s$ satisfying (2) and (3). Let

$$S(\ell) = \sum_{n_1=1}^{N} \dots \sum_{n_s=1}^{N} e(\ell Q(n_1,\dots,n_s)) . \tag{11}$$

Let

$$L = [2c_4(s)^{-1}(N / \log N)^{c_3(s)}] \tag{12}$$

where $c_4(s)$ is sufficiently large, then from Lemma 1 of Chapter 1 we have

$$\sum_{\ell=1}^{L} |S(\ell)| > N^s/6. \tag{13}$$

Let ℓ be a natural number , $1 \leq \ell \leq L$, having

$$|S(\ell)| \gg N^s / L . \tag{14}$$

We define linear forms $L_1,\dots,L_s$ with symmetric coefficient matrix via the identity

$$Q(x_1,\dots,x_s) = x_1 L_1(\underline{\underline{x}}) + \dots + x_s L_s(\underline{\underline{x}}) . \tag{15}$$

Then there are integers $x_1,\dots,x_h$ not all zero, with

$$Q(x_1,\dots,x_h) \equiv 0 \pmod{m}, \tag{6}$$

and having

$$|x_i| \le K_i \qquad (i = 1,\dots,h). \tag{7}$$

The case $K_1 = \dots = K_h = m^{(1/2)+(1/2h)}$ is Theorem 1 of [7].

Proof. We first observe that the result is trivial if $K_i \ge m$ for some i; hence we suppose that

$$K_i < m \qquad (i = 1,\dots,h) \tag{8}$$

Clearly we may assume that $m > 1$, and that m is square free. For any m may be written in the form

$$m = r^2 a$$

where a is square free. If $K_1 \dots K_h \ge m^{(h+1)/2}$, then $(K_1/r)\dots(K_h/r) \ge a^{(h+1)/2}$. A solution $(y_1,\dots,y_h)$ of $Q(y) \equiv 0 \pmod{a}$, with $|y_i| \le K_i/r$, yields a solution $x_i = ry_i$ of (5) satisfying (7).

Let $d = (h-1)/2$. According to [7], for every prime p dividing m there are integer vectors $\underset{=}{r}_1^{(p)},\dots,\underset{=}{r}_d^{(p)}$ which are linearly independent modulo p, and for which

$$Q(s_1 \underset{=}{r}_1^{(p)} + \dots + s_d \underset{=}{r}_d^{(p)}) \equiv 0 \pmod{p}$$

whenever $s_1,\dots,s_d$ are integers. By the Chinese remainder theorem there are integer vectors $\underset{=}{r}_1,\dots,\underset{=}{r}_d$ having

$$\underset{=}{r}_i \equiv \underset{=}{r}_i^{(p)} \pmod{p},$$

for each prime p dividing m. Write $\underset{=}{r}_i = (r_{i1},\dots,r_{ih})$.

By Minkowski's linear forms theorem, and taking account of (5), there are integers $s_1,\dots,s_d$, $z_1,\dots,z_h$ not all zero, with

Let $M_1,\dots,M_s$ be the first s successive minima of the convex body described by

$$|2\ell\, L_j(\underline{x}) - x_{s+j}| < N^{-1} \qquad (j = 1,\dots,s),$$

$$|x_j| < N$$

with respect to the integer lattice in $2s$ - dimensional space. It is established in the proof of Lemma 5 of [3] that

$$|S(\ell)|^2 \leq c_6(s)(M_1\dots M_s)^{-1} N^s (\log N)^s .$$

In view of (14), then,

$$(M_1\dots M_s)^{-1} \geq c_7(s)\, L^{-2} N^s (\log N)^{-s} \tag{16}$$

We now consider the cases of odd and even s separately.

Case I. Odd s. By the definition of successive minima, we can find s linearly independent integer vectors $\underline{r}'_\mu$ in $2s$ - dimensional space with

$$|2\ell\, L_j(\underline{r}_\mu) - r_{j+s,\mu}| < N^{-1} M_\mu , \tag{17}$$

$$|r_{j\mu}| < NM_\mu \tag{18}$$

for $j = 1,\dots,s$, $\mu = 1,\dots,s$. Here $\underline{r}'_\mu = (r_{1\mu},\dots,r_{2s,\mu})$ and $\underline{r}_\mu = (r_{1\mu},\dots,r_{s\mu})$.

Let us write

$$K_\mu = c_7(s)^{-1/s} L^{2/s} (2\ell)^{(s+1)/2s} M_\mu^{-1} (\log N) N^{-1} , \tag{19}$$

then

$$K_1\dots K_s \geq (2\ell)^{(s+1)/2} \tag{20}$$

from (16). We also write

$$\theta_{\mu\nu} = 2\ell \sum_{j=1}^{s} r_{j\mu} L_j(\underline{r}_\nu) \qquad (\mu,\nu = 1,\dots,s),$$

so that

$$\|\theta_{\mu\nu}\| < s M_\mu M_\nu \tag{21}$$

from (17) and (18). Let $b_{\mu\nu}$ be integers with

$$\| \theta_{\mu\nu} \| = |\theta_{\mu\nu} - b_{\mu\nu}| \qquad (\mu,\nu = 1,\dots,s) . \tag{22}$$

By Lemma 1 and (20) there are integers $x_1,\dots,x_s$ not all zero, with

$$| x_\mu | \leq K_\mu \qquad (\mu = 1,\dots,s) \tag{23}$$

and

$$\sum_{\mu=1}^{s} \sum_{\nu=1}^{s} b_{\mu\nu} x_\mu x_\nu \equiv 0 \pmod{2\ell} . \tag{24}$$

Put $n_i = \sum_{\mu=1}^{s} r_{i\mu} x_\mu$ for $i = 1,\dots,s$. Then

$$Q(n_1,\dots,n_s) = \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} \Big(\sum_{i=1}^{s} L_i(\underline{r}_\mu) r_{i\nu} \Big) x_\mu x_\nu$$

$$= (2\ell)^{-1} \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} \theta_{\mu\nu} x_\mu x_\nu$$

$$= (2\ell)^{-1} \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} b_{\mu\nu} x_\mu x_\nu + (2\ell)^{-1} \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} (\theta_{\mu\nu} - b_{\mu\nu}) x_\mu x_\nu . \tag{25}$$

The first sum on the right hand side of (25) is an integer, in view of (24). Thus

$$\| Q(n_1,\dots,n_s) \| \leq (2\ell)^{-1} \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} \| \theta_{\mu\nu} \| \, |x_\mu| |x_\nu|$$

$$< \frac{s}{2\ell} \sum_{\mu=1}^{s} \sum_{\nu=1}^{s} M_\mu M_\nu K_\mu K_\nu$$

$$= \frac{s^3}{2\ell} (c_7(s))^{-2/s} L^{4/s} (2\ell)^{(s+1)/s} (\log N)^2 N^{-2}$$

from (21) and (23). For sufficiently large $c_4(s)$, we have

$$\| Q(n_1,\dots,n_s) \| < 2s^3 (c_7(s))^{-2/s} L^{5/s} (N/\log N)^{-2}$$

$$< L^{-1} .$$

Moreover, we have

$$|n_i| = \Big| \sum_{\mu=1}^{s} r_{i\mu} x_\mu \Big| \le s M_\mu N K_\mu$$

$$\le s c_7(s)^{-1/s} L^{2/s} (2\ell)^{(s+1)/2s} \log N$$

$$\le 2s c_7(s)^{-1/s} L^{(s+5)/2s} \log N < N.$$

By hypothesis, then, we must have

$$(n_1,\dots,n_s) = \underline{0},$$

so that $\sum_{\mu=1}^{s} x_\mu \underline{r}_\mu = \underline{0}$ and consequently

$$\sum_{\mu=1}^{s} x_\mu L_j(\underline{r}_\mu) = \underline{0} \qquad (j = 1,\dots,s). \tag{26}$$

Combining (26) with (17) we obtain

$$\Big| \sum_{\mu=1}^{s} x_\mu r_{j+s,\mu} \Big| < N^{-1} \sum_{\mu=1}^{s} M_\mu |x_\mu|$$

$$\le N^{-1} \sum_{\mu=1}^{s} M_\mu K_\mu < 1$$

as we already saw above. Hence

$$\sum_{\mu=1}^{s} x_\mu r_{j\mu} = 0$$

is true not only for $j = 1,\dots,s$ but for $j = s+1,\dots,2s$ also. This contradicts the linear independence of $\underline{r}_1',\dots,\underline{r}_\mu'$.

Thus the theorem is proved in Case I .

Case II. Even s . From (16) and $M_1 \le \dots \le M_s$, we obtain

$$(M_1 \dots M_{s-1})^{-1} \ge c_7(s)^{(s-1)/s} L^{-2(s-1)/s} (N/\log N)^{s-1}. \tag{27}$$

Let $\underline{r}_\mu'$, $\underline{r}_\mu$, $\theta_{\mu\nu}$, $b_{\mu\nu}$ be as in Case I. By repeating the argument of Case I , with $s-1$ instead of s , we obtain integers $x_1,\dots,x_{s-1}$ such that

$$\sum_{\mu=1}^{s-1} \sum_{\nu=1}^{s-1} b_{\mu\nu} x_\mu x_\nu \equiv 0 \pmod{2\ell}$$

and

$$|x_\mu| \leq H_\mu = c_8(s)\, L^{2/s}\, (2\ell)^{s/2(s-1)}\, M_\mu^{-1} (\log N) N^{-1}.$$

After all,

$$H_1 \ldots H_{s-1} \geq (2\ell)^{((s-1)/2) + 1/2)}$$

provided that $c_8(s)$ is sufficiently large. Let

$$(n_1, \ldots, n_s) = \sum_{\mu=1}^{s-1} x_\mu \underline{r}_\mu' .$$

Continuing as before, we obtain for $\| Q(n_1, \ldots, n_s) \|$ the upper bound

$$\frac{s^3}{2\ell} \Big(\max_{1 \leq \mu \leq s-1} H_\mu M_\mu \Big)^2 \leq c_9(s)\, L^{(4/s)+(1/(s-1))} (\log N)^2 N^{-2}$$

$$< L^{-1}, \qquad (28)$$

and

$$\max (|n_1|, \ldots, |n_s|) \leq s \max_{1 \leq \mu \leq s-1} H_\mu M_\mu N$$

$$\leq c_{10}(s)\, L^{(2/s) + (s/2(s-1))} \log N < N, \qquad (29).$$

for a suitable choice of $c_4(s)$. The argument used in Case I can be repeated to obtain

$$\sum_{\mu=1}^{s-1} x_\mu \underline{r}_\mu' = \underline{0},$$

which is a contradiction. This proves the theorem in Case II.

4. Quadratic forms with "free" variables

Here we suppose that

$$Q(n_1,\ldots, n_s) = Q'(n_1,\ldots, n_{s-m}) + \sum_{i=1}^{m} \alpha_i n_{s-m+i}^2 ,$$

the last m variables being termed "free", for obvious reasons.

THEOREM 2 *Let $\varepsilon > 0$, $Q(n_1, \ldots, n_s)$ a quadratic form with m free variables, and suppose that $N > N(\varepsilon, s)$. Then there exist integers, not all zero, bounded in absolute value by N and having*

$$\| Q(n_1,\ldots, n_s) \| < N^{-c(s,m) + \varepsilon}$$

where $c(s,m)$ is the maximum over r in $0 \leq r \leq m$, $r \equiv s + 1 \pmod 2$ of

$$2 - \frac{6 + 2^{2 - r}}{(s-r) + 5} . \tag{30}$$

Remarks Supposing m to be sufficiently large in terms of s we may choose r asymptotically equal to $\log s$ to obtain

$$c(s,m) = 2 - 6/s + O(1/s^2).$$

In particular, for $m \geq 2$ we have $c(5,m) = 9/8$ and $c(11,m) = 3/2$.

Proof We make only one alteration to the proof of Theorem 1 (working as in case I since we have made $s - r$ to be odd). We suppose r is chosen so that (30) is maximised. We assume the theorem is false and obtain, as before,

$$\sum_{\ell=1}^{L} |S(\ell)| >> N^S . \tag{31}$$

Here $L = N^{c(s,m) + \varepsilon}$.

Now let

$$A_i(\ell) = \left| \sum_{n=1}^{N} e(\alpha_i \ell n^2) \right| \qquad (i = 1,\ldots,m)$$

and

$$S'(\ell) = \left| \sum_{n_1=1}^{N} \cdots \sum_{n_{s-m}=1}^{N} e(Q'(n_1,\ldots,n_{s-m})) \right| \prod_{i=r+1}^{m} A_i(\ell) .$$

Since we have assumed the theorem is false, by Dirichlet's theorem there are integers q_i with $\| q_i\alpha_i \| < (LN)^{-1}$ with $N \leq q_i \leq LN$ $(i = 1,\dots,r)$, having the associated a_i coprime to q_i. So, by Lemma 2 of Chapter 1 we have

$$\sum_{\ell=1}^{L} A_i^2(\ell) \ll LN^{1+\delta},$$

and, using the trivial inequality $A_i(\ell) \leq N$,

$$\sum_{\ell=1}^{L} A_i^{2^h}(\ell) \ll LN^{2^h - 1 + \delta} \qquad (32)$$

for $h = 1, 2, \dots$.

A repeated application of Cauchy's inequality to (31) yields

$$\prod_{i=1}^{r} \Big(\sum_{\ell=1}^{L} A_i(\ell)^{2^i} \Big)^{2^{r-i}} \sum_{\ell=1}^{L} S'(\ell)^{2^r} \gg N^{s2^r}.$$

This with (32) gives, for at least one ℓ, that

$$S'(\ell)^2 \gg N^{2(s-r) + 2(1-2^{-r})}L^{-2}N^{-2\delta}$$

We write $t = s - m + r - 1$. Working as in section 3 we find that

$$\prod_{i=1}^{s-m} M_i^{-1} \prod_{i=t}^{s} M_i^{-1} \gg N^{s-r+2(1-2^{-r})-3\delta}L^{-2}.$$

Hence, putting $\delta = \varepsilon/4$ we obtain

$$L^{(s-r+1)/2} \prod_{i=1}^{s-m} M_i \prod_{i=t}^{s} M_i \ll 1.$$

This indicates that we can find integers $n_1,\dots, n_{s-m}, n_t,\dots, n_s$ with

$$\| Q(n_1,\dots,n_{s-m},0,0,\dots,0,n_t,\dots,n_s) \| < N^{-c(s,m)+\varepsilon}.$$

This is the desired contradiction which completes the proof.

THEOREM 3 Given $\varepsilon > 0$ and a quadratic form Q in five variables, at least two of which are free. Then, for infinitely many N there is a

a solution of the inequality

$$|| Q(n_1,\ldots,n_5) || \quad < \quad N^{-8/7 + \varepsilon}$$

with $0 < \max |n_i| \leq N$.

Remarks By using a result of Hooley's [5] we could replace N^{ε} by a small power of $\log N$. W. M. Schmidt has shown that for almost all additive forms in five variables one may take the exponent as $-2 + \varepsilon$ and the result is valid for all $N > N(Q,\varepsilon)$. We shall be considering his method in Chapter Three. Before proving Theorem 3 we require one more lemma which, as far as the present author is aware, is new and may have other applications :

LEMMA 3 Let L, N be natural numbers with $L > N \geq 1$. Suppose α is real, with $| q\alpha - a | < q^{-1}$, $(a,q) = 1$. We write

$$S(\ell) = \Big| \sum_{n=1}^{N} e(\alpha \ell n^2) \Big|.$$

Then

$$\sum_{\ell=1}^{L} S(\ell)^4 \ll N^2 (\log N)^2 \max \left(\frac{LN^2}{q}, N^2, q, L \right)$$

Remarks This result is superior to the case $h = 2$ of (32) if $N \leq q \leq NL$ or $N^2 < q < L$.

Proof Let $\rho(n)$ denote the number of solutions in x,y of $x^2 + y^2 = n$ subject to $1 \leq x \leq N$, $1 \leq y \leq N$. Then

$$\sum_{\ell=1}^{L} S(\ell)^4 = \sum_{\ell=1}^{L} \Big| \sum_{n=1}^{2N^2} \rho(n)\, e(\alpha \ell n) \Big|^2 .$$

We now divide up the range of summation over ℓ into at most $(3L/q + 1)$ blocks of $q/2$ consecutive integers. Let B be one such block. From the hypothesis on α we see that for $\ell, m \in B$, $\ell \neq m$ we have

$$|| (m - \ell)\alpha || > (2q)^{-1}.$$

By the well-known large sieve inequality [6] we see that

$$\sum_{\ell \in B} \Big| \sum_{n=1}^{2N^2} \rho(n)\, e(\alpha \ell n) \Big|^2 \leq 2(N^2 + q) \sum_{n=1}^{2N^2} \rho(n)^2 \qquad (33).$$

Now the last sum on the right of (33) is just the number of solutions in integers of

$$u^2 + v^2 = x^2 + y^2$$

subject to $1 \leq u,v,x,y \leq N$. It is well known that this number is $\ll N^2 (\log N)^2$. Thus

$$\sum_{\ell \in B} S(\ell)^4 \ll N^2 (\log N)^2 \max (N^2, q).$$

So, altogether we have

$$\begin{aligned} \sum_{\ell=1}^{L} S(\ell)^4 &\ll (3Lq^{-1} + 1) N^2 (\log N)^2 \max (N^2, q) \\ &\ll N^2 (\log N)^2 \max (LN^2 q^{-1}, N^2, q, L) \end{aligned}$$

and the proof is complete.

Proof of Theorem 3 We write

$$Q(n_1,\ldots,n_s) = Q'(n_1,n_2,n_3) + \alpha_1 n_4^2 + \alpha_2 n_5^2$$

The proof is trivial if α_1 is rational, so we assume it to be irrational. Let a/q be a convergent to the continued fraction of α_1. There are infinitely many since α_1 is irrational. Let

$$N = q^{2/3}, \quad L = N^{8/7 - \varepsilon}$$

and suppose q is sufficiently large. We work as in the proof of Theorem 2, but by Lemma 3 we note that

$$\sum_{\ell=1}^{L} \Big| \sum_{n=1}^{N} e(\alpha_1 n^2 \ell) \Big|^4 \ll N^{4 + \delta}$$

Hence

$$\sum_{\ell=1}^{L} S'(\ell) = \sum_{\ell=1}^{L} \Big| \sum_{\substack{n_1,n_2,\\ n_3}} e(Q'(n_1,n_2,n_3)\ell) \Big|^4 \gg N^{14} - 2\delta L^{-2}.$$

Thus, for at least one ℓ,

$$S'(\ell) \gg N^{7/2 - \delta/2} L^{-\frac{3}{4}}.$$

The proof may now be easily completed as in the case of theorems 1 & 2.

5. Related results

It is appropriate here to note that Schlickewei [8] has obtained a similar result for an additive form of kth powers using a method of W. M. Schmidt [9]. The exponent of N here satisfies

$$c(s) = -k + O((\log s)^{-\frac{1}{2}}).$$

It would be highly desirable to have some argument analogous to the one used in section 2 for kth powers which would enable one to get $c(s) = -k + O(s^{-1})$. The result of Theorem 1 and Schlickewei's result have been extended by R.C. Baker and myself to simultaneous approximation [1b]. We proved :

THEOREM 4 *Let* $N \geq 1$. *Given Quadratic forms* $Q_1(x_1,\ldots,x_s),\ldots,$ $Q_h(x_1,\ldots,x_s)$ *where* $s \geq c(h, \varepsilon)$, *there exist integers* $n_1,\ldots,n_s$ *with* (2), *having*

$$\| Q_i(n_1,\ldots,n_s) \| < N^{-(2/h) + \varepsilon} \qquad (i = 1,\ldots,h).$$

THEOREM 5 *Let* $N \geq 1$, *and let* $F_1,\ldots,F_h$ *be additive forms of* kth *powers in* s *variables with* $s \geq c'(k,h,\varepsilon)$. *Then there exist non-negative integers* $n_1,\ldots, n_s$ *with* (2), *having*

$$\| F_i(n_1,\ldots,n_s) \| \leq N^{-(k/h) + \varepsilon} \qquad (i = 1,\ldots,h).$$

References to Chapter Two

1. R.C. Baker & G. Harman, "Small fractional parts of Quadratic forms" J. Edinburgh Math. Soc.

1b. ————————, "Small fractional parts of quadratic and additive forms", Math. Proc. Camb. Phil. Soc. 90 (1981) 5 - 12.

2. I. Danicic, "An extension of a theorem of Heilbronn", Mathematika 5 (1958), 30-37 .

3. H. Davenport, "Indefinite quadratic forms in many variables (II)", Proc. London Math. Soc. (3) 8 (1958), 109-126.

4. H. Davenport and D. Ridout, "Indefinite quadratic forms", ibid. 9 (1959), 544-555.

5. C. Hooley, "On a new technique and its applications to the theory of numbers", ibid. 38 (1979), 115-151.

6. H.L. Montgomery, "The analytic principle of the large sieve", Bull. Amer. Math. Soc. 84 (1978), 547-567.

7. A. Schinzel, H.-P. Schlickewei and W.M. Schmidt, "Small solutions of quadratic congruences and small fractional parts of quadratic forms", Acta Arithmetica 37 (1980) 241 - 248

8. H.-P. Schlickewei, "On indefinite diagonal forms in many variables" J. Reine angew. Math. 307/8 (1979), 279-294.

9. W.M. Schmidt, "Small zeros of additive forms in many variables", Trans. Amer. Math. Soc. 248 (1979), 121-133

where $f(s) \sim \sqrt{2s}$ as $s \to \infty$. Schmidt makes explicit for which particular set $\underline{A}$ of almost all s-tuples c may be taken this large. It is the set of "not very well approximable s-tuples" (henceforth 'n.v.w.a.') in the sense that

$$\prod_{i=1}^{s} || \alpha_i n || > C(\varepsilon,\alpha)\, n^{-1-\varepsilon} \qquad (2)$$

for every natural n and every $\varepsilon > 0$. Examples of such sets of numbers include s-tuples of real algebraic numbers with $1, \alpha_1, \ldots, \alpha_s$ linearly independent over the rationals [6] and s distinct rational powers of e [1]. We shall show in section 3 how to prove, for $k \geq 2$, that

$$c_k(s) \geq f(s) \qquad \text{where } f(s) \sim \sqrt{ks},$$

by modifying Schmidt's argument. Of course the exponent obtained seems to be rather artificial. It would be reasonable to conjecture that $c_k(s) >> s$ (implied constant depending on k).

The problem with $k = 1$ is very interesting, and here the present state of knowledge is quite satisfactory. As shown above, the exponent may not be improved beyond 1 without any further assumption on $\underline{\alpha}$. Schmidt has shown [7] that if $1, \alpha, \beta$ are linearly independent over the rationals and ε is an arbitrary positive number, then there are infinitely many pairs x,y with $x > 0$, $y > 0$ and with

$$|| \alpha x + \beta y || < \varepsilon(\max(x,y))^{-\mu} \qquad (3)$$

where $\mu = (\sqrt{5} + 1)/2 = 1.61803 \ldots$ In the same paper he also demonstrates the existence of s real numbers $\alpha_1, \ldots, \alpha_s$ with $1, \alpha_1, \ldots, \alpha_s$ linearly independent over the rationals and with

$$|| \alpha_1 x_1 + \ldots + \alpha_s x_s || > C(\varepsilon)\, (\max(x_1, \ldots, x_s))^{-2-\varepsilon}$$

for $\varepsilon > 0$, $x_1, \ldots, x_s$ positive integers. The situation is rather

CHAPTER THREE RESULTS FOR ALMOST ALL FORMS

1. In this chapter $F_k^j(n_1,\ldots,n_s)$ ($j = 1,2$; $k \geq 1$) shall denote additive forms with

$$F_k^1(n_1,\ldots,n_s) = \alpha_1 n_1^k + \ldots\ldots + \alpha_s n_s^k$$

and

$$F_k^2(n_1,\ldots,n_s) = \alpha_1|n_1^k| + \ldots\ldots + \alpha_s|n_s|^k$$

Let $c_k^j(s)$ denote the supremum of numbers c such that

$$\sup_{F_k^j} \min_{0<|\underline{n}|<N} \left|\left| F_k^j(\underline{n}) \right|\right| < N^{-c+\varepsilon} \qquad \text{for } N > N(\varepsilon).$$

Here we have written $\underline{n} = (n_1,\ldots,n_s)$ and $|\underline{n}| = \max(|n_1|,\ldots,|n_s|)$. By Dirichlet's Theorem $c_1^1(s) \geq s$ and the ε may be dispensed with. Of course, in actual fact $c_1^1(s) = s$. Obviously, for even k, $c_k^1 = c_k^2$. For all k the example $\alpha_i = \sqrt{2}$ ($i = 1,\ldots,s$) shows that $c_k^2(s) \leq k$. The situation is very different for $c_k^1(s)$ when k is odd (see [9]). As mentioned at the end of chapter 2, it is known [5] that $c_k^2(s) = k + O((\log s)^{-\frac{1}{2}})$. Now let us write $\underline{\alpha} = (\alpha_1,\ldots,\alpha_s)$ and $\underline{A}$ for a set in R^s such that $\mu(R^s/\underline{A}) = 0$. Here μ is the normal Lebesgue measure on R^s. Each set $\underline{A}$ contains "almost all" points $\underline{\alpha}$, according to the standard definition of "almost all". We write $H(A)$ for the set of additive forms $F_k^2(\underline{n})$ such that $\underline{\alpha} \in \underline{A}$. We now define $c_k(s)$ to be the supremum of numbers c such that

$$\inf_{\underline{A}} \sup_{F_k^2 \in H(A)} \min^{*}_{0<|\underline{n}|\leq N} N^{c-\varepsilon} \left|\left| F_k^2(\underline{n}) \right|\right| < 1 \qquad (1)$$

where the $*$ indicates that the minimum holds for all $N > N(F_k^2,\varepsilon)$. A result of W.M. Schmidt (Theorem 20B of [8]) shows that

$$c_2(s) > f(s)$$

different, however, if we only ask for $\underline{\underline{\alpha}}$ to be n.v.w.a. In that case we have the following generalization of Kronecker's Theorem :

THEOREM 1 *Let* $\varepsilon > 0$. *Suppose* $\underline{\underline{\alpha}}$ *is n.v.w.a. Then, for any real* β, *and* $N > N_0(\varepsilon, \underline{\underline{\alpha}})$ *there are positive integers* $n_1,\dots,n_s$ *with*

$$n_i \leq N \qquad (i = 1,\dots,s) \tag{4}$$

having

$$\| F_1^2(\underline{\underline{n}}) + \beta \| < N^{-s+\varepsilon} . \tag{5}$$

We note that the above result is best possible apart from the N^{ε} factor.* Whether it is possible to relax the condition on $\underline{\underline{\alpha}}$ remains an open question, though the result in [7] shows that the gap in our knowledge is quite narrow.

2. Proof of Theorem 1

The proof shall be by contradiction and, apart from Lemma 1 of Chapter One and the simple result

$$\Big| \sum_{m=1}^{M} e(\gamma m) \Big| \ll \| \gamma \|^{-1} ,$$

is quite elementary, only using a double application of the box principle. The proof was inspired by Chapter 20 of [8] although the details here are quite different. We write

$$L = N^{s-\varepsilon} + 1 , \quad S(\ell) = \prod_{i=1}^{s} \sum_{n_i=1}^{N} e(\alpha_i \ell n_i) .$$

Assuming the theorem to be false, by Lemma 1 of Chapter One

$$\sum_{\ell=1}^{L} | S(\ell) | >> N^s .$$

Thus there is a number B and a set Q such that

* See [4].

$$B \gg N^{\varepsilon}, \tag{6}$$

$$|S(\ell)| > B \quad \text{for } \ell \in Q, \tag{7}$$

also

$$B|Q| \gg N^{s}(\log N)^{-1}. \tag{8}$$

From (7) we find that

$$\prod_{i=1}^{s} ||\alpha_i \ell|| \ll B^{-1} \quad \text{for } \ell \in Q. \tag{9}$$

Put $M = [\log_2 B]$. We assume N_0 is so large that $N_0^{\varepsilon/2} > (s \log N_0)^s$. If $|Q| < N^{\varepsilon/2}$ it can be deduced from (8), (9) that there is an integer $\ell < N^s$ with

$$\ell \prod_{i=1}^{s} ||\alpha_i \ell|| \ll N^{-\varepsilon/2}(\log N),$$

which contradicts (2) for N sufficiently large. We may thus assume that $|Q| \geq N^{\varepsilon/2}$. Put

$$v_i(\ell) = \min(M, [-\log_2 ||\alpha_i \ell||]) \tag{10}$$

and

$$\underline{v}(\ell) = (v_1(\ell), \ldots, v_s(\ell)).$$

We now split Q into M^s subsets (some of which may be empty) $A(\underline{t})$, where the coordinates of $\underline{t}$ are positive integers not exceeding M. To this end we write

$$A(\underline{t}) = \{\ell : \ell \in Q, \ \underline{v}(\ell) = \underline{t}\}.$$

Given $\underline{t}$ with $\max_i t_i = M$, then (say $t_h = M$), if $\ell_1, \ell_2 \in A(\underline{t})$, then

$$\prod_{i=1}^{s} ||\alpha_i(\ell_1 - \ell_2)|| < ||\alpha_h(\ell_1 - \ell_2)|| \leq ||\alpha_h \ell_1|| + ||\alpha_h \ell_2|| \ll B^{-1} \tag{11}$$

using the definition of t_h, M.

Given $\underline{t}$ with $\max_i t_i < M$ and $\ell_1, \ell_2 \in A(\underline{t})$ then

$$\prod_{i=1}^{s} || \alpha_i \ell_{j(i)} || \ll \max_{k=1,2} \prod_{i=1}^{s} || \alpha_i \ell_k || \qquad (12)$$

Here $j(i)$ is any function taking only the values 1 and 2. (This follows since

$$\frac{1}{2} < \frac{|| \alpha_i \ell_1 ||}{|| \alpha_i \ell_2 ||} < 2 \ ).$$

Hence

$$\prod_{i=1}^{s} || \alpha_i (\ell_1 - \ell_2) || \leq \prod_{i=1}^{s} (|| \alpha_i \ell_1 || + || \alpha_i \ell_2 ||)$$

$$\ll \max_{k=1,2} \prod_{i=1}^{s} || \alpha_i \ell_k || \ll B^{-1} \qquad (13)$$

using (9) and (12).

From a simple application of the box principle we deduce there is one $\underline{\underline{t}}$ with

$$| A(\underline{\underline{t}}) | \geq \frac{| Q |}{M^s} \gg \frac{Q}{(s \log N)^s} > 1 .$$

From a second application of the box principle, there are two integers $\ell_1, \ell_2 \in A(\underline{\underline{t}})$ with

$$| \ell_1 - \ell_2 | \ll \frac{(s \log N)^s L}{| Q |} . \qquad (14)$$

Put $r = | \ell_1 - \ell_2 |$. Combining (11), (13), (14) we have that

$$r \prod_{i=1}^{s} || \alpha_i r || \ll \frac{L (s \log N)^s}{B | Q |} \ll N^{-\varepsilon} (s \log N)^{s+1}$$

$$\ll N^{-\varepsilon/2} (\log N).$$

This contradicts the definition of n.v.w.a. (i.e. (2)) providing N is sufficiently large, since $r < N^s$. The proof of Theorem 1 is thus complete.

3. A Generalization of Schmidt's Result

Here we prove a lemma by adapting the proof of Theorem 20 B of [8] . It is also in the form of a quantitative generalization of Kronecker's Theorem. We first require the following notation :

A function is said to satisfy T(A, G, D, E) if there exist positive constants A, G, D, E, such that for any $\delta > 0$, any real α and $N > N_0(\delta, A, G, D, E)$ the inequality

$$\left| \sum_{n=1}^{N} e(\alpha f(n)) \right| = C > N^{1 - E + \delta}$$

implies the existence of a natural number q with $q < N^{\delta}(N/C)^{A}$,

$$|| \alpha q || < N^{\delta}(N/C)^{D} N^{-G}.$$

LEMMA 1 Let f satisfy T(A, G, D, E), let $\underline{\alpha}$ be n.v.w.a. and β an arbitrary real number. Suppose $s \geq s_0(A, G, D, E)$. Let $N > N_1(\varepsilon, \underline{\alpha}, A, G, D, E)$. Then there are natural numbers $n_1, \ldots n_s$ with $n_i \leq N$ and

$$|| \alpha_1 f(n_1) + \ldots + \alpha_s f(n_s) + \beta || < N^{-c(s) + \varepsilon} \qquad (15)$$

where $c(s) = Gh$. Here h is the largest integer with $h^2 A + D'h \leq s$, $D' = \max(A, D)$. In particular $c(s) \sim G\sqrt{s/A}$.

Proof We assume the lemma is false, so by Lemma 1 of Chapter One,

$$\sum_{m=1}^{L} \prod_{i=1}^{s} | S_i(m) | \gg N^{s}. \qquad (16)$$

Here $L = N^{c(s) - \varepsilon}$, $S_i(m) = \sum_{n=1}^{N} e(\alpha_i m f(n))$.

From (16) we deduce that there is a subset Q of the integers $1, \ldots,$ L and a number B such that

$$2B > \prod_{i=1}^{s} |S_i(m)| \geqq B \qquad \text{for } m \in Q,$$

and

$B|Q| >> N^s (\log N)^{-1}$. Hence there are numbers C_i and a subset Q' of Q such that

$$C_i \leq |S_i(m)| < 2C_i \qquad \text{for } m \in Q' \quad (i=1,..s),$$

and

$$B \leq \prod_{i=1}^{s} C_i \ll B, \quad \text{while} \quad |Q'| B >> N^s (\log N)^{-s-1}.$$

Without loss of generality, $C_1 \geq C_2 \geq \ldots \geq C_s$. Clearly, if $s_0(A, G, D, E)$ is sufficiently large, we have that

$$C_i > N^{1 - E+\delta} \quad \text{for } i = 1,\ldots, h.$$

Since f satisfies $T(A, G, D, E)$, for each $m \in Q'$ there are integers $r_i = r_i(m)$ $(i = 1,\ldots, h)$ with

$$r_i < (N/C_i)^A N^{\delta},$$

and

$$||\alpha_i r_i m|| < N^{D - G + \delta} C_i^{-D}.$$

We choose $\delta = \varepsilon/4h^2$. We put $q = q(m) = r_1 \ldots r_h$, then

$$q \leq N^{h(A + \delta)} B^{-hA/s},$$

while

$$||\alpha_i mq|| \ll N^{D - G + A(h - 1) + h\delta} B^{-hA/s} C_i^{A-D}.$$

Now, since the number of divisors of mq is $\ll N^{\delta}$, as m runs through Q' we deduce that $>> N^s B^{-1} N^{-\delta}$ different numbers mq arise. By the box principle there is an integer z with

$$z \ll (N^s B^{-1} N^{-\delta})^{-1} L N^{h(A + \delta)} B^{-hA/s} \qquad (17)$$

and having

$$z \prod_{i=1}^{h} || \alpha_i z || \ll z \prod_{i=1}^{h} (N^{D - G + A(h-1) + h\delta_B - hA/s} C_i^{A-D}). \quad (18)$$

If $A \leq D$ we note that $\prod_{1}^{h} C_i \gg B^{h/s}$, thus the right hand side of (18) is

$$\ll LN^{Ah^2 + h(D-G) - s + \varepsilon/2} B^{1 - h^2A/s - Dh/s}$$

$$\ll LN^{-Gh + \varepsilon/2} \quad \text{since } B \ll N^s$$

$$\ll N^{-\varepsilon/2}. \quad (19).$$

Since by (17) z is bounded by a power of N, (19) contradicts the definition of $\underline{\alpha}$ being n.v.w.a. for $N > N(\underline{\alpha}, \varepsilon)$.

If $A > D$ we work similarly to the above, but use $\prod_{i=1}^{h} C_i \ll N^h$. This completes the proof of this lemma.

We now note the values of A, G, D, E associated with two certain functions :

	A	G	D	E	c(s)
I) f(n) is the nth prime	2	1	2	4/5	$\sqrt{s/2}$
II) $f(n) = n^k + g(n)$	k	k	k	2^{1-k}	$\sqrt{ks}$

In II) g(n) is an arbitrary polynomial of degree k-1. The result for I) comes from [10], that for II) comes from Theorem 3 of [2]. Results for powers of primes or polynomials in a prime variable may be deduced from the theorems of Chapter 4. It is interesting that on the Generalized Riemann Hypothesis $f(p_n) = p_n^k$ satisfies T(2,k,k,E) for some $E > 0$, which is a stronger condition than is given in II) for $g(n) = 0$, and gives $c(s) \sim k\sqrt{s/2}$, so a fortiori this holds for II) in the case $g(n) = 0$ on the GRH. It should be noted that the parameters D, E do not enter into the asymptotic formula for c(s),

the important fact is how the rational approximation to α and the estimate for the exponential sum are linked when E is very small (but not arbitrarily small).

4. A simultaneous approximation problem with primes

The following theorem follows on from the previous work of this chapter in that it involves n.v.w.a. s-tuplets and uses a similar method of proof :

THEOREM 2 *Let* $\underline{\alpha}$ *be a* n.v.w.a. *s-tuplet of real numbers, and* $(\beta_1,\ldots,\beta_s)$ *any real s-tuplet. Suppose* $\varepsilon > 0$ *is given, and* $N > N(\underline{\alpha},\varepsilon)$. *Then there is a solution of*

$$\max_{1 \leq i \leq s} \| \alpha_i p + \beta_i \| < N^{-1/(2s(s+1))} + \varepsilon \qquad (20)$$

with

$$2 \leq p \leq N. \qquad (21)$$

Remarks The case $s = 1$ is, of course, due to R.C. Vaughan [11], and in this case one only needs the hypothesis α_1 irrational. We may thus suppose in the following proof that $s \geq 2$. We note that for the case $s = 2$ we get the exponent $-1/12 + \varepsilon$.

Proof The proof shall be by contradiction. We write $\delta = \varepsilon/8$,

$$A(\underline{k}) = \alpha_1 k_1 + \ldots + \alpha_s k_s \quad \text{for} \quad \underline{k} = (k_1,\ldots,k_s),$$

$$L = N^{1/(2s(s+1))} - \varepsilon/2, \qquad S(\underline{k}) = \Big| \sum_{p \leq N} (\log p)\, e(pA(\underline{k})) \Big| .$$

By a standard argument (see Chapter 15 of [8]) if (20) has no solution subject to (21) then

$$\sum_{\substack{\underline{k} \neq 0 \\ |\underline{k}| \leq L}} S(\underline{k}) \gg N.$$

Now there is a set Q of points $\underline{\underline{k}}$ with B members (note that $B < N^{1/6}$) such that

$$S(\underline{\underline{k}}) \gg N(B \log N)^{-1} \quad \text{for every } \underline{\underline{k}} \in Q.$$

We now use the result quoted in I) of section 3 to find that for every $\underline{\underline{k}} \in Q$ there is a $q(\underline{\underline{k}})$ with

$$|| q(\underline{\underline{k}}) A(\underline{\underline{k}}) || \ll N^{-1+\delta} B^2$$

and

$$q(\underline{\underline{k}}) \ll B^2 N^{\delta}.$$

Since the number of divisors of $q(\underline{\underline{k}})k_i$ is $\ll N^{\delta}$, there are $\gg BN^{-\delta}$ distinct points $q(\underline{\underline{k}})\,\underline{\underline{k}}$ with

$$|| q(\underline{\underline{k}}) A(\underline{\underline{k}}) || \ll N^{-1+\delta}.$$

There are thus two points a distance $\ll B^2 N^{\delta} L (BN^{-\delta})^{-1/s}$ apart. Write $\underline{\underline{n}}$ for the difference between two such points. Then

$$|| A(\underline{\underline{n}}) || \ll N^{-1+\delta} \tag{22}$$

with

$$|\underline{\underline{n}}| \ll B^2 N^{\delta} L (BN^{-\delta})^{-1/s}, \tag{23}$$

Now, by a classical transference theroem (see Chapter 5 of [3]), since $\underline{\underline{\alpha}}$ is n.v.w.a. if (23) holds then

$$\begin{aligned} || A(\underline{\underline{n}}) || &\gg (B^2 N^{\delta} L (BN^{-\delta})^{-1/s})^{-s-\delta} \\ &\gg B^{-2s+1} L^{-s} N^{-2s\delta} \\ &\gg N^{-1+\delta} B^2 (N^{1-3s\delta} B^{-1-2s} L^{-s}). \end{aligned} \tag{24}$$

Now $B^{-1-2s} L^{-s} N^{1-3s\delta} > N^{-(1+2s)/2(s+1) - 1/2(s+1) + \varepsilon s/2 + 1 - 3s\delta}$ $> N^{\delta}$. Hence (24) contradicts (22) for N sufficiently large and the proof is complete.

References to Chapter Three

1. A. Baker, "On some Diophantine Inequalities involving the exponential function." Can. J. Math. 17 (1963), 616 - 627.

2. R.C. Baker, "Weyl Sums and Diophantine Approximation," J. London Math. Soc. (2), 25 (1982), 25-34

3. J.W.S. Cassels, An introduction to Diophantine Approximation, Cambridge Tracts in Math. and Math. Physics, no. 45 (1957)

4. H. Davenport & W.M. Schmidt, "Dirichlet's Theorem on diophantine approximation", Acta Arithmetica XVI (1970) 413-424.

5. H.-P. Sclickewei, "On indefinite diagonal forms in many variables" J. Reine angew. Math. 307/8 (1979), 279-294.

6. W.M. Schmidt, "Simultaneous approximation to algebraic numbers by rationals," Acta Math. 125, 189-201. (1970).

7. ————, "Two questions in Diophantine Approximation", Monatshefte für Mathematik 82 (1976), 237-245.

8. ————, Small fractional parts of polynomials , Amer. Math. Soc. Providence R.I., 1977

9. ————, "Diophantine inequalities for forms of odd degree." Advances in Math. 38 (1980), 128-151.

10. R.C. Vaughan, "Sommes trigonometriques sur les nombres premiers ", C.R. Acad. Sci. Paris, Serie A 285 (1977) 981-983.

11. ————, "The distribution of αp modulo one", Mathematika 24, (1977) 136-141.

Chapter Four TRIGONOMETRIC SUMS OVER PRIMES

Much of the work of this chapter is contained in two papers by the present author [5, 6]. Only Theorem 7 has not previously appeared. We shall prove here the following results :

THEOREM 1. Suppose $\varepsilon > 0$ is given. Let $f(x)$ be a real valued polynomial in x of degree $k \geq 2$. Put

$$\gamma = 4^{1-k}.$$

Suppose α is the leading coefficient of f and there are integers a, q such that

$$|q\alpha - a| < q^{-1} \quad \text{with} \quad (a,q) = 1 . \tag{1}$$

Then we have

$$\sum_{p \leq N} (\log p)\, e(f(p)) \ll N^{1+\varepsilon} \left(\frac{1}{q} + \frac{1}{N^{\frac{1}{2}}} + \frac{q}{N^k} \right)^{\gamma} \tag{2}$$

THEOREM 2. Let $f(x)$ be a real polynomial in x of degree $k \geq 2$, with irrational leading coefficient. Suppose $\varepsilon > 0$ is given. Then there are infinitely many solutions of

$$\| f(p) \| < p^{-\gamma/2 + \varepsilon} \tag{3}$$

where γ is given in Theorem 1.

THEOREM 3 Let k be an integer ≥ 3, and $\varepsilon > 0$. Suppose

$N^{1-1/k} \leq q \leq N^{k/2}$, $|\alpha q - a| < N^{-k/2}$, $(a, q) = 1$. Then

$$\left| \sum_{p \leq N} (\log p)\, e(\alpha p^k) \right| \ll N^{1+\varepsilon-\gamma} \tag{4}$$

where $\gamma = (k 2^k)^{-1}$.

THEOREM 4 For $\varepsilon > 0$, β an arbitrary real number and α irrational there are infinitely many solutions of the inequality

$$\| \alpha p^k + \beta \| < p^{-\xi+\varepsilon}. \tag{5}$$

Here $\xi = (2^{k+1} + (2^{k+1} - 1 - 2k)/k)^{-1}$ and $k \geq 3$.

THEOREM 5 Let k be an integer ≥ 4 and $f(x)$ a real polynomial in x with irrational leading coefficient. Then, for a given $\varepsilon > 0$, there are infinitely many solutions of the inequality

$$\| f(p) \| < p^{-\tau+\varepsilon} \tag{6}$$

Here, for $k \leq 11$,

$$\tau = (2T + (2^{k+1} - 1 - 2k)/k)^{-1}$$

where T is defined by the following table:

k	4	5	6	7	8	9	10	11
T	46	110	240	414	672	1080	1770	3000

For $k \geq 12$ we have

$$\tau = (12\,[k^2(\log k + {}^1/_2 \log\log k + 1{\cdot}3)])^{-1}$$

THEOREM 6 Suppose f is a real polynomial of degree $k \geq 2$ with an irrational leading coefficient. Then, for $\varepsilon > 0$, there are infinitely many solutions of

$$\| f(P_2) \| < P_2^{-\sigma+\varepsilon} \tag{7}$$

where $\sigma = (2^k + 2)^{-1}$.

THEOREM 7 Let $\varepsilon > 0$, $k \geq 3$. Suppose α is real with

$$| q\alpha - a | < \min(q^{-1}, N^{-k/2}) \qquad (a,q) = 1.$$

Then

$$\Big| \sum_{p \leq N} (\log p)\, e(\alpha p^k) \Big| \ll N^{1+\varepsilon} Q^{-1} . \qquad (8)$$

Where

$$Q = q^{2^{-k}/(k-1)} \quad \text{if } q < N^{1-k^{-1}}$$

$$= N^{(k2^k)^{-1}} \quad \text{if } N^{1-k^{-1}} \leq q \leq N^{k/2 - 1/k + \frac{1}{2}}$$

$$= (q^{-1} N^{k+\frac{1}{2}})^{2^{-k}} \quad \text{if } N^{(k+1)/2 - 1/k} < q \leq N^{k/2 - 2^{-k-1} + \frac{1}{2}}$$

As already remarked in Chapter One, these improve results of I.M. Vinogradov. We use an identity of R.C. Vaughan's to convert sums over primes into double sums, but it should be noted that it is essentially no stronger than Vinogradov's method (see Chapter 9 of [17] for example). The results of Theorems 1 and 2 are shown for the special case αp^2 by A. Ghosh [3]. He also quotes a result for αp^3 which is weaker than (2). The previous best result is due to Vinogradov who obtained the exponent

$$(4^{k+1}(k+1))^{-1}$$

in place of γ when k is small. For large k he showed [16] that this expression may be improved to $(25\, k^2\, (2 + \log k))^{-1}$. We shall improve the method of that paper to establish Theorems 3-5 and 7. The result of Theorem 3 is included in that of Theorem 7 and they improve upon Theorem 1 for $k \geq 3$ when the added conditions in their statement are satisfied. An application of these theorems is given in Chapter Five. In some circumstances the requirements of Theorems 3 and 7 will not be met and then the weaker result of Theorem 1 must be used instead.

If f is a monomial and α is rational, then Theorems 1,3 & 7 can be substantially improved. It follows from Theorem 2 of [11] that

$$\sum_{p \leq N} (\log p)\, e\left(\frac{ap^k}{q}\right) \ll q^{\varepsilon} (\log N)^{7/2} (N^{\frac{1}{2}} q^{\frac{1}{2}} + N q^{-\frac{1}{2}} + N^{\frac{3}{4}} q^{\frac{1}{8}})$$

The proof of this result requires the use of L-series. Elementary proofs of such results had earlier been given by Vinogradov [15] and Chen [2]. Vinogradov obtained the estimate for $q < N^{2/9}$, while Chen showed that

$$\sum_{p \leq N} e\left(\frac{ap^k}{q}\right) \ll N^{2/3+\varepsilon} q^{1/3} \quad \text{for } q \geq N^{\frac{5}{8}}.$$

It seems interesting that an elementary proof of a result nearly as strong as that which follows from Theorem 2 of [11] is possible improving on the results of [2,15]. By ameliorating Vinogradov's analysis, or by adapting the method of [13] one can prove such a result, but with $N^{\frac{3}{4}}q^{\frac{1}{8}}$ weakened to $N^{5/6}$.

No result of the type given in Theorem 6 seems to have appeared in the literature before, although S.W. Graham has shown [4] that there are infinitely many solutions of

$$\| \alpha P_2 \| < P_2^{-1/3} (\log P_2)^{18}$$

His method is an application of the small sieve. In section 4 we show that the exponent of $\log P_2$ may be reduced to 4/3 using the large sieve inequality. For large k it follows from Chapter 5 of [17], with only slight modifications, that one can get the same answer for $f(P_2)$ as the best currently known results for $f(n)$. In particular, one can modify the details of [1] to obtain

$$\sigma = (2(\log k + 1)(3.25 + (k+1)\log(k(\log k + 1)))/(\log k))^{-1}$$

which is better than the present result for $k \geq 7$. Of course we have, a fortiori, that there are infinitely many solutions of

$$\| \alpha n^k \| < n^{-\sigma+\varepsilon}$$

for α irrational. This is apparently a new result for large k, improving upon previous results by a factor of 4.

2. Proof of Theorems 1 & 2

In this section the method is to estimate double sums by applying the Weyl differencing technique $2(k-1)$ times, that is $k-1$ times to each variable. The application to one variable is implicit in Lemma 2, the application to the other is given explicitly in Lemma 3. The weakness of the results of Theorems 1 & 2 is due to the need to apply the differencing to both variables. The working here is substantially as given in [5], though here some details are appended concerning the discrepancy of the sequence αp^k.

LEMMA 1 *For any real valued function* f *and natural number* N *we have*

$$\sum_{p \le N} (\log p)\, e(f(p)) = O\left(N^{\frac{1}{2}}\right) + S_1 - S_2 - S_3 \tag{9}$$

where

$$S_1 = \sum_{d \le N^{1/3}} \mu(d) \sum_{\ell < Nd^{-1}} (\log \ell)\, e(f(d\ell))$$

$$S_2 = \sum_{r \le N^{2/3}} \phi_1(r) \sum_{m \le Nr^{-1}} e(f(rm))$$

$$S_3 = \sum_{N^{1/3} < m \le N^{2/3}} \phi_2(m) \sum_{N^{1/3} < n \le Nm^{-1}} \Lambda(n)\, e(f(mn))$$

and

$$\phi_1(r) \ll \log r\,, \quad \phi_2(m) \ll \tau(m) \tag{10}$$

Proof This is essentially given in [12]. See also [13]. This result is usually refered to as Vaughan's Identity. In the above $\mu(d)$ is the Mobius function and $\tau(d)$ denotes the number of divisors of d.

LEMMA 2. Let $g(x)$ be a real valued polynomial of degree k with leading coefficient β. Then, for $\varepsilon > 0$,

$$\Big| \sum_{n=1}^{X} e(g(n)) \Big|^R \ll X^{R-k+\varepsilon} \sum_{y=1}^{(k!)X^{k-1}} \min\left(X, \frac{1}{\|\beta y\|}\right)$$

Here $R = 2^{k-1}$.

Proof This is Lemma 2 of Chapter One restated here for convenience.

We require the following notation in the proof of Lemma 3:

$$\Delta_y (f(x)) = f(x + y) - f(x),$$

and define a differencing operator inductively by

$$\Delta_{y_1 \ldots y_t} f(x) = \Delta_{y_t} (\Delta_{y_1 \ldots y_{t-1}} f(x)).$$

For a function $\psi(m)$ write

$$\underline{\Psi}(n, y_1, \ldots y_s) =$$

$$\underline{\psi}(n) \prod_{i=1}^{s} \underline{\psi}(n + y_i) \prod_{1 \le i < j \le s} \underline{\psi}(n + y_i + y_j) \ldots\ldots \prod_{i=1}^{s} \underline{\psi}\Big(n + \sum_{j \ne i} y_i\Big) \underline{\psi}\Big(n + \sum_{i=1}^{s} y_i\Big)$$

We note that there are 2^s terms in the above product. In the remainder of this section we suppose $f(x) = \underline{\alpha} x^k + \underline{\beta} x^{k-1} + \ldots + \underline{\omega}$.

LEMMA 3 Let $f(x)$ be as given in Theorem 1. Suppose $\underline{\varepsilon} > 0$, and $\underline{\phi}(u)$, $\underline{\psi}(v)$ are real functions. Put

$$T = \max |\underline{\psi}(v)|$$

$$F = \Big(\frac{1}{W} \Big(\sum_{u \le W} \underline{\phi}^2(u) \Big)\Big)^{\frac{1}{2}}$$

For positive integers M, W, X write

$$S = \sum_{\substack{u=1 \\ uv \leq M}}^{W} \sum_{v=1}^{X} \underline{\phi}(u)\, \underline{\psi}(v)\, e(f(uv)) \tag{11}$$

Then

$$\left(\frac{S}{TF}\right)^{R^2} \ll (WX)^{R^2} (X^{-R} + (WX)^{-k+\varepsilon} \sum_{z=1}^{Y} \min\left(W, \frac{1}{\|\underline{\alpha} z\|}\right)) \tag{12}$$

where $Y = X^k W^{k-1} (k!)^2$ and $R = 2^{k-1}$.

Proof

Without loss of generality we may assume $T = F = 1$ and $\underline{\psi}(v) \geq 0$ for all v. For the moment we shall ignore the condition $uv \leq M$ in (11). By Cauchy's inequality

$$S^2 \ll W \sum_{v_1=1}^{X} \sum_{v_2=1}^{X} \underline{\psi}(v_1)\, \underline{\psi}(v_2) \sum_{u=1}^{W} e(f(uv_1) - f(uv_2))$$

$$\leq 2W \operatorname{Re} S_1 + E_1 \tag{13}$$

Here, for a positive integer s,

$$S_s = \sum_{y_1=1}^{X-1} \cdots \sum_{y_s=1}^{X-1} \sum_{n} \underline{\Psi}(n, y_1, \ldots y_s) \sum_{u=1}^{W} e(\Delta_{y_1} \cdots_{y_s} f(un)), \tag{14}$$

the range of summation over n being $1 \leq n < n + y_1 + \ldots + y_s \leq X$, the differencing operator acts on n not u, and

$$E_s = W^{2^s} X^{2^s - 1}. \tag{15}$$

It is easily shown by induction, using Cauchy's inequality as we did to obtain (13), that

$$S^{2^s} \ll E_s + W^{2^{s-1}} X^{2^s - s - 1} |S_s| \tag{16}$$

LEMMA 4 Suppose we have the hypotheses of Lemma 3 and its Corollary, but either

$$\underline{\phi}(x) = 1 \quad \underline{\text{for all}} \quad x$$

or $$\underline{\phi}(x) = \log x \quad \underline{\text{for all}}\ x,$$

Then

$$S \ll (XW)^{1+\underline{\varepsilon}}\, X^{(k-1)/R}\, (q^{-1} + q(WX)^{-k} + W^{-1})^{R^{-1}}, \tag{20}$$

Proof The $\log x$ factor may easily be removed by partial summation so we presume that $\phi(x) \equiv 1$. Again we may ignore the condition $u v \leq M$. By the hypotheses of this lemma together with Hölder's inequality and Lemma 2 we have

$$S^R \ll X^{\varepsilon/2 + R-1} \sum_{v=1}^{X} \sum_{y=1}^{(k!)W^{k-1}} W^{R-k+\varepsilon/2} \min\left(W, \frac{1}{\|\alpha y v^k\|}\right)$$

$$\ll (XW)^{3\varepsilon/4}\, X^{R-1}\, W^{R-k} \sum_{z=1}^{(k!)W^{k-1}X^k} \min\left(W, \frac{1}{\|\alpha z\|}\right)$$

The estimate (20) follows easily.

Proof of Theorem 1 By Lemma 1 there are $\ll \log N$ sums to estimate of the form

$$\sum_{u=1}^{N/X} \underline{\phi}(u) \sum_{\substack{v=X \\ uv \leq N}}^{2X} \underline{\psi}(v)\, e(f(uv)) \tag{21}$$

where $X < N^{\frac{1}{2}}$, and $\phi(u) \equiv 1$ or $\log u$ if $X \leq N^{1/3}$. We estimate (21) by the corollary to Lemma 3 if

$$X^R \geq \min(N^{\frac{1}{2}}, q, N^k q^{-1})$$

and by Lemma 4 otherwise. The theorem follows observing that $(1 - (k-1)/R) \geq \gamma R$.

for $s = 2, \ldots k-1$.

We write

$$S'(n, y_1, \ldots, y_{k-1}) = \sum_{u=1}^{W} e(\Delta_{y_1 \ldots y_{k-1}} f(un)). \qquad (17)$$

As is well known (Lemma 10 B of [10]),

$$\Delta_{y_1 \ldots y_{k-1}} f(un) = y_1 \ldots y_{k-1} \left(\tfrac{1}{2} k! \underline{\alpha} u^k (2n + y_1 + \ldots + y_{k-1}) + (k-1)! \underline{\beta} u^{k-1}\right)$$

$$= u^k h(y_1 \ldots y_{k-1}, n) + u^{k-1}(k-1)! \underline{\beta}\, y_1 \ldots y_{k-1} \quad \text{say.}$$

We now combine (14) - (17) (with $s = k-1$) with Lemma 2 to obtain (18):

$$S^{R^2} \ll (WX)^{R^2} X^{-R} + (WX)^{R^2-k} \sum_{y_1} \ldots \sum_{y_{k-1}} \sum_{n} \sum_{z=1}^{k! W^{k-1}} W^{\varepsilon/2} \min\left(W, \frac{1}{\|z h(y_1 \ldots y_{k-1}, n)\|}\right)$$

Now the number of ways of writing a number $t \leq X^k W^{k-1} (k!)^2$ as a product of the form

$$\tfrac{1}{2} y_1 y_2 \ldots y_k (k!)(2n + y_1 + \ldots + y_{k-1}) = t$$

is $\ll (WX)^{\varepsilon/2}$. Thus (12) follows from (18).

The added condition $uv \leq M$ in (11) only causes problems with notation, not technical difficulties in the above proof. The range of summation over u in (17) will depend on $M, n, y_1, \ldots, y_{k-1}$ but this does not affect the estimate of Lemma 2, since the range for u will still be over no more than W consecutive integers.

COROLLARY Let S be as in (11) and let a, q be as in (1). If $T = o(X^{\delta})$, $F = o(X^{\delta})$ for every $\delta > 0$, then

$$S \ll (XW)^{1+\underline{\varepsilon}} (X^{-R} + W^{-1} + q^{-1} + (XW)^{-k} q)^{\underline{\gamma}}, \qquad (19)$$

Proof This follows easily from (12).

Proof of Theorem 2 Let

$$S_\ell = \sum_{N^{\frac{1}{2}} \le p \le N} \log p \, e(\ell f(p)) .$$

Then, by Lemma 1, we may estimate $\sum_{\ell=1}^{L} |S_\ell|$ by obtaining an upper bound for sums of the form

$$\sum_{\ell=1}^{L} \left| \sum_{u=1}^{W} \underline{\phi}(u) \sum_{v=X}^{2X} \underline{\psi}(v) \, e(\ell f(uv)) \right| .$$

$$uv \le N$$

We may estimate this sum from Lemma 3 if

$$X \ge \min(N^{1/2R}, q^{1/k}, NL^{1/k} q^{-1/k}).$$

Otherwise we may add an extra summation range over ℓ in Lemma 4. In either case we get the bound

$$\ll (NL)^{1+\epsilon/2} (q^{-1} + N^{-\frac{1}{2}} + q N^{-k} L^{-1})^{\gamma} . \qquad (22)$$

Now if α, the leading coefficient of f, is irrational there are infinitely many convergents a/q to its continued fraction. Let a/q be one such convergent with q sufficiently large. Put $N = q^2$, $L = N^{\gamma/2-\epsilon}$. Then, by (22), combining the $O(\log N)$ sums,

$$\sum_{\ell=1}^{L} S_\ell < \frac{N}{10}$$

if q is large enough. The result now follows easily from Lemma 1 of Chapter One since this gives a solution of (3) with $N^{\frac{1}{2}} \le p \le N$ and N tends to infinity with q.

The discrepancy of αp^k We say α is of type μ if there is a constant $C(\alpha,\varepsilon)$ such that

$$|| q\alpha || > q^{-\mu-\varepsilon} C(\alpha, \varepsilon) \qquad (23)$$

for all integers q. By this definition almost all integers are of type 2, including all real algebraic numbers (by the Thue-Siegel-Roth Theorem). We write

$$D_N(\alpha_n) = \sup_{I \subset [0,1)} \left| \sum_{\substack{1 \le n \le N \\ \{\alpha_n\} \in I}} 1 - n|I| \right|$$

Then, using the Erdős-Turán Theorem (Theorem 2.5 of [8]) we have

$$D_N(f(p_n)) \ll_{\alpha,\varepsilon} N^{1-\gamma/2+\varepsilon} \qquad (24)$$

if the leading coefficient of f is α where α is of type $\mu \le 2k-1$. Looking forward to the results of the next section we may prove

$$D_N(\alpha p^k) \ll_{\alpha,\varepsilon} N^{1-\xi+\varepsilon} \qquad (25)$$

if α is of type 2. If α is of type > 2 results may be obtained using Theorem 7's method.

3. Some lemmas required for the proof of Theorems 3-7

We first observe (working as in [13]) that the result of Lemma 1 remains unaltered if we add the condition that all variables summed over in S_1, S_2, S_3 are coprime to some integer q with $\log q \ll \log N$. We shall denote such a condition by writing Σ'. The improvements of this section come mainly from relating double sums to integrals of sums in accordance with Vinogradov's method (see Lemmas 9 & 10), although we will make somenew refinements here. We are also able to give good bounds for certain subsums by making quite stringent assumptions on the diophantine approximation to α (Lemma 7). The working of this section is substantially as given in [6], although lemma 9 in the present account is more general than the corresponding result in [6] .

It follows, as in section 2, that we need only estimate two types of sum (after applying partial summation to S_1 of Lemma 1) :

$$\text{(I)} \qquad \sum_{Y<y\leq 2Y}{}' \underline{\psi}(y) \sum_{x\leq Ny^{-1}}{}' \underline{\phi}(x)\, e(f(xy)) \tag{26}$$

where $N^{1/3} \leq Y \leq N^{1/2}$.

$$\text{(II)} \qquad \sum_{Y<y\leq 2Y}{}' \underline{\psi}(y) \sum_{x\leq Ny^{-1}}{}' e(f(xy)) \tag{27}$$

Here $Y < N^{1/3}$. Both $\underline{\phi}$ and $\underline{\psi}$ in (7) and (8) can be assumed to satisfy

$$\underline{\phi}(u) \ll u^{-\delta}, \quad \underline{\psi}(v) \ll v^{-\delta} \tag{28}$$

for every $\delta > 0$.

LEMMA 5 For any positive integers W, q and real number ρ we have , for $\varepsilon > 0$,

$$\Big|\sum_{u=1}^{W}{}' e(\underline{\rho}\, u^k)\Big|^R \ll \max_{\substack{d|q \\ \mu(d)\neq 0 \\ d\leq W}} (Wq)^{\underline{\varepsilon}} \left(\frac{W}{d}\right)^{R-k} \sum_{z=1}^{J} \min\left(\frac{W}{d}, \frac{1}{\|\underline{\rho}\, z\|}\right). \tag{29}$$

Here $R = 2^{k-1}$ and $J = (k!)\, d\, W^{k-1}$.

We remark that by the conventional method of estimating sums of the type which occurs on the right of (29), the estimate is a decreasing function of d. Thus d can essentially be thought of as 1 in (29). This gives the usual Weyl inequality result, but we have removed all numbers from the sum on the left of (29) not coprime to q.

PROOF It is easily shown (see Lemma 2 Chapter 9 of [17]) that

$$\sum_{u=1}^{W}{}' e(\underline{\rho}\, u^k) = \sum_{d|q} \underline{\mu}(d)\, S(d) \tag{30}$$

where

$$S(d) = \begin{cases} 0 & \text{if } d > W \\ \displaystyle\sum_{u=1}^{[Wd^{-1}]} e(\underline{\rho}\, u^k d^k) & \text{for } d \leq W. \end{cases} \tag{31}$$

By Lemma 2,

$$|S(d)|^R \ll W^{\underline{\varepsilon}/2} \left(\frac{W}{d}\right)^{R-k} \sum_{z=1}^{(k!)(W/d)^{k-1}} \min\left(\frac{W}{d}, \frac{1}{\|\underline{\rho} z d^k\|}\right). \tag{32}$$

$$\ll W^{\underline{\varepsilon}} \left(\frac{W}{d}\right)^{R-k} \sum_{z=1}^{J} \min\left(\frac{W}{d}, \frac{1}{\|\underline{\rho}\, z\|}\right)$$

Combining (30), (31) and (32) gives (29) since the number of divisors of q is $\ll q^{\underline{\varepsilon}}$. Similarly we may prove

$$\sum_{\ell=1}^{L} \Big|\sum_{u=1}^{W}{}' e(f(u))\Big|^R \ll \max_{\substack{d|q \\ \mu(d)\neq 0 \\ d\leq W}} (LWq)^{\underline{\varepsilon}} \left(\frac{W}{d}\right)^{R-k} \sum_{z=1}^{X} \min\left(\frac{W}{d}, \frac{1}{\|\underline{\alpha}\, z\|}\right) \tag{33}$$

where $X = (k!)\, d\, L\, W^{k-1}$, and $f(u) = \underline{\alpha} u^k + \ldots + \underline{\omega}$.

LEMMA 6. *Suppose* $Y \leq N^{1/2}$, $1 \leq m \leq k$, $|q\,\underline{\alpha} - a| < q^{-1}$, $(a, q) = 1$. *Then, for* $\varepsilon > 0$,

$$\sum_{Y<y\leq 2Y}{}' \underline{\psi}(y) \sum_{x\leq Ny^{-1}}{}' \underline{\phi}(x)\, e(\underline{\alpha} y^k x^k) \tag{34}$$

$$\ll F N^{1+\varepsilon} \left(\left(\frac{Y^{k-m+1}}{N} \right)^{2^{2-m-k}} + \left(Y^{k-m} \left(\frac{1}{q} + \frac{q}{N^k} \right) \right)^{2^{2-m-k}} + \underline{\delta}_m Y^{2^{1-m}} \right),$$

where $\underline{\phi}(x)$, $\underline{\psi}(y)$ *are real valued functions;* $\underline{\phi}(x) \equiv 1$ *is an additional necessary condition if* m *is taken as* 1. *Here*

$$\underline{\delta}_m = \begin{cases} 0 & \text{if } m = 1 \\ 1 & \text{otherwise} \end{cases}$$

and

$$F = \max_u |\underline{\phi}(u)| \max_v |\underline{\psi}(v)| . \tag{35}$$

Proof For $m = 1$ this is Lemma 4, while for $m=k$ it is the corollary to Lemma 3. When $1 < m < k$ the result follows by applying the Weyl differencing technique only for the variable y $m-1$ times in Lemma 3, i.e. stopping the induction at $s = m - 1$. For all k Lemma 5 must be used in place of Lemma 2.

Henceforth in this chapter the letter F is reserved for the expression given in (35).

LEMMA 7. *Suppose* $Y \leq N^{1/2}$, $|\underline{\alpha} - a/q| \leq (N^k L)^{-1}$, $(a, q) = 1$, $N > L \geq 1$. *Put*

$$S_L = \sum_{\ell=1}^{L} \Big| \sum_{Y< y <2Y}{}' \underline{\psi}(y) \sum_{x\leq Ny^{-1}}{}' \underline{\phi}(x)\, e(\underline{\alpha}\, \ell\, (xy)^k) \Big|$$

Then, if $\underline{\phi}(x) = 1$ *for all* x,

$$S_L \ll F(NL)^{1+\varepsilon}\left(\frac{Y}{N}+\frac{1}{q}+\frac{q}{L}\left(\frac{Y}{N}\right)^k\right)^{2^{1-k}}. \tag{36}$$

Otherwise

$$S_L \ll F(NL)^{1+\varepsilon}\left(\frac{1}{Y^{1/2}}+\left(\frac{qY^k}{N^kL}+\frac{Y^k}{q}+\frac{Y}{N}\right)^{2^{-k}}\right). \tag{37}$$

Proof We write

$$S_L = \sum_{\ell=1}^{L} A_\ell$$

and prove (36) first. By partial summation

$$A_\ell = \sum_{Y<y\leq 2Y}{}' \left(\sum_{x\leq Ny^{-1}} \underline{\delta}_y(x)\, S_{x,y}(\ell) + \psi(y)\, e(\underline{\alpha}'\ell y^k ([Ny^{-1}]+1)^k)\, S_{[Ny^{-1}],y}(\ell)\right).$$

Here $\underline{\delta}_y(x) = \underline{\psi}(y)\, e(\underline{\alpha}'\ell(yx)^k) - \underline{\psi}(y)\, e(\underline{\alpha}'\ell(x+1)^k y^k)$, $\underline{\alpha}' = \underline{\alpha} - aq^{-1}$

and $$S_{x,y}(\ell) = \sum_{n\leq x}{}' e\left(\frac{a\ell(ny)^k}{q}\right)$$

Clearly $\underline{\delta}_y(x) \ll F\ell y^k x^{k-1}(LN^k)^{-1}$. Thus

$$\sum_{\ell=1}^{L}|A_\ell| \ll \sum_{Y<y\leq 2Y}{}' \left(\sum_{x\leq N/y} \frac{Fy^k x^{k-1}}{N^k} \sum_{\ell=1}^{L}|S_{x,y}(\ell)| + F\sum_{\ell=1}^{L}|S_{[Ny^{-1}],y}(\ell)|\right) \tag{38}$$

By (33), the fact that $(y,q)=1$ and Holder's inequality we find that

$$\sum_{\ell=1}^{L}|S_{x,y}(\ell)| \ll (Lx)^{1+\varepsilon/2}\left(\frac{1}{x}+\frac{1}{q}+\frac{q}{x^kL}\right)^{2^{1-k}} \tag{39}$$

It is now easy to deduce (36) from (38) and (39).

To prove (37) we use Cauchy's inequality to obtain

$$|A_\ell|^2 \leq \left(\sum_{x\leq NY^{-1}} \underline{\phi}(x)^2\right)\left(\sum_{x\leq NY^{-1}} \sum_{Y<v_1<H_x} \underline{\psi}(v_1) \sum_{Y<v_2<H_x} \underline{\psi}(v_2)\, e(\underline{\alpha}\, x^k \ell(v_1^k - v_2^k))\right)$$

where $H_x = \min(2Y, Nx^{-1})$

$$\leq \frac{N}{Y} \max_u |\underline{\phi}(u)|^2 S_\ell \quad , \text{ say.} \tag{40}$$

We now remove all the terms with $v_1 = v_2$ from S_ℓ to leave a sum A'_ℓ say. The terms with $v_1 = v_2$ contribute

$$\ll \max_v |\underline{\psi}(v)|^2 N$$

to S_ℓ and hence

$$\ll \frac{FNL}{Y^{1/2}} \tag{41}$$

to S_L. We proceed to estimate A'_ℓ as we treated A_ℓ above. We now get sums $S_{x,y_1,y_2}(\ell)$ to estimate given by

$$S_{x,y_1,y_2}(\ell) = \sum_{n \leq x}{}' e\left(\frac{a\ell n^k (y_1^k - y_2^k)}{q}\right).$$

The complication arises that $y_1^k - y_2^k$ may not be coprime to q. It turns out that quite a crude argument will suffice for the applications (the $Y^k q^{-1}$ term in (37) can be improved but not the $q Y^k N^{-k} L^{-1}$ term). We have

$$(q, (y_1^k - y_2^k)) \leq |y_1^k - y_2^k| \ll Y^k ;$$

thus

$$\sum_{\ell=1}^{L} |S_{x,y_1,y_2}(\ell)| \ll (Lx)^{1+\varepsilon} \left(\frac{1}{x} + \frac{Y^k}{q} + \frac{q}{x^k L}\right)^{2^{1-k}}.$$

Hence

$$\sum_{\ell=1}^{L} A'_\ell \ll \max_v |\underline{\psi}(v)|^2 Y (LN)^{1+\varepsilon} \left(\frac{Y}{N} + \frac{Y^k}{q} + \frac{qY^k}{N^k L}\right)^{2^{1-k}} \tag{42}$$

A combination of (40), (41) and (42) together with Cauchy's inequality then yields (37) as desired. We note that there are no technical difficulties involved in replacing $\underline{\alpha} n^k$ by a polynomial of degree k with leading coefficient $\underline{\alpha}$.

$$\sum_{Y<y\leq 2Y}{}' \psi(y) \sum_{x\leq Ny^{-1}}{}' \phi(x)\, e(\alpha_{\underline{\ell}} y^k x^k) \ll FN^{1+\varepsilon}\left(\frac{1}{Y}+\frac{\lambda}{q}\right)^{2^{-k}}\left(1+\quad H\quad\right)^{2^{-k}}. \qquad (46)$$

Here $\underline{\lambda} = (\ell,q)$ and $H = LY^k Q^{-1} + q(Y/N)^k$.

Proof. Without loss of generality $Y = 2^t$ where t is an integer. Some notation is required inorder to split the trigonometric sum in (26) into subsums. We define sets of integers C_m as follows for $0 \leq m \leq t$: $C_0 = \{Y\}$, $C_m = \{ y_m : y_m = Y + rY2^{1-m},\ 0 \leq r \leq 2^{m-1}\}$. We put $Y_m = Y.2^{-m}$, and write $\theta(y_m)$ for the set of integers x with $N(y_m + 2Y_m)^{-1} < x \leq N(y_m + Y_m)^{-1}$ for $m > 0$. We define $\theta(y_0)$ as the set of integers x with $0 < x \leq N(2Y)^{-1}$. Clearly

$$\sum_{Y<y\leq 2Y}{}' \psi(y) \sum_{x\leq N/y}{}' \phi(x)\, e(\alpha_{\underline{\ell}} y^k x^k) = \sum_{m=0}^{t} \sum_{y_m \in C_m} S(y_m) + O(N/y) \qquad (47)$$

where

$$S(y_m) = \sum_{y=y_m+1}^{y_m+Y_m}{}' \psi(y) \sum_{x\in\theta(y_m)}{}' \phi(x)\, e(\alpha_{\underline{\ell}} x^k y^k). \qquad (48)$$

We write $S_{\underline{\ell}}(y)$ for the inner sum in (28). We shall consider m fixed at the moment and concentrate on one subsum $S(y_m)$. In the following the summation over x will be for $x \in \theta(y_m)$. We note that there are $\ll NY_m/Y^2$ numbers in $\theta(y_m)$, and $\ll Y/Y_m$ numbers in C_m.

Write

$$X = NY^{-1}.$$

We now relate $S_{\underline{\ell}}(y)$ to integrals in accordance with one of Vinogradov's methods. We make one important change in that we will use an infinite series of integrals rather than one integral plus an error. The saving this apparent innovation produces is only significant for small k ; it makes no real difference to the result of Theorem I of Chapter 6 of [17], for instance. We have

LEMMA 8 Let $\phi(x)$ be an arbitrary function. Let B and A be positive integers. Then, for $\delta > 0$, we have

$$I = \int_0^1 \Big| \sum_{A<u\leq A+B} \phi(u)\, e(y u^k) \Big|^{2^k} dy \ll B^{2^k - k + \delta} \max_{A<u\leq A+B} |\phi(u)|^{2^k} . \qquad (43)$$

Proof

$$I = \sum_{0<u_1\leq B} \cdots \sum_{0<u_{2^k}\leq B} \prod_{j=1}^{2^{k-1}} \phi(u_j) \prod_{j=2^{k-1}+1}^{2^k} \overline{\phi}(u_j) \int_0^1 e(y F(u_1,\ldots,u_{2^k}))dy \qquad (44)$$

where $F(u_1,\ldots,u_{2^k}) = \sum_{j=1}^{2^{k-1}} (u_j+A)^k - \sum_{j=2^{k-1}+1}^{2^k} (u_j+A)^k$.

As the integral in (44) is either 0 or 1 we may conclude that

$$I \leq \max_{A<u\leq A+B} |\phi(u)|^{2^k} \sum_{0<u_1\leq B} \cdots \sum_{0<u_{2^k}\leq B} \int_0^1 e(yF(u_1,\ldots,u_{2^k}))dy$$

$$= \max_{A<u\leq A+B} |\phi(u)|^{2^k} \int_0^1 \Big| \sum_{0<u\leq B} e(y(u+A)^k) \Big|^{2^k} dy \qquad (45)$$

The estimate $B^{2^k-k+\delta}$ for the integral in (45) is well known (see Theorem 4 of [7]) and completes the proof of this lemma.

We remark now that the drawback of the results of Lemmas 6 and 7 is that their estimates become trivial for Y near $N^{\frac{1}{2}}$ (in fact the situation is even worse in Lemma 6 for small m). The following lemma deals with estimation of sums where both ranges are quite large.

LEMMA 9 Let $Y \leq N^{\frac{1}{2}}$, $\ell \leq L \leq N$. Put $Q = \max(q, (N^k L)^{\frac{1}{2}})$ and suppose that $|\alpha q - a| < Q^{-1}$, $(a,q) = 1$, $\varepsilon > 0$. Then

$$|S_\ell(y)|^{2^k} \ll \sum_{r=0}^{\infty} \frac{X^{-rk2^k}\, Ir(y) X^k}{r!}, \tag{49}$$

where

$$Ir(y) = \int_{\mathfrak{J}(y)} \Big| \sum_x{}' x^{rk}\, e(ux^k)\, \underline{\phi}(x) \Big|^{2k} du. \tag{50}$$

Here

$$\mathfrak{J}(y) = [\underline{\alpha} y^k \ell - \frac{X^{-k}}{2}, \ \underline{\alpha} y^k \ell + \frac{X^{-k}}{2}].$$

(The reader familiar with Vinogradov's work should note that we have been able to make $\mathfrak{J}(y)$ somewhat larger than usual; this requires us to use an infinite series but it will become apparent that this is no real problem).

To obtain (49), note that for any u,

$$S_\ell(y) = \sum_x{}' \underline{\phi}(x)\, e(ux^k)\, e(x^k(\underline{\alpha} y^k \ell - u))$$

$$= \sum_x{}' e(ux^k) \sum_{r=0}^{\infty} \frac{x^{kr}\, (\underline{\alpha}\, y^k \ell - u)^r\, (2\pi i)^r}{r!} \underline{\phi}(x)$$

The interchanges of orders of summation and integration in the following working are easily justified. We have

$$S_\ell(y) = X^k \int_{\mathfrak{J}(y)} \sum_{r=0}^{\infty} \sum_x{}' \frac{e(x^k u)\, x^{kr}\, (\alpha y^k \ell - u)^r\, (2\pi i)^r\, \phi(x)}{r!}\, du$$

$$= \sum_{r=0}^{\infty} \frac{(2\pi i)^r X^k}{r!} \int_{\mathfrak{J}(y)} (\alpha y^k \ell)^r \sum_x{}' e(x^k u)\, x^{kr} \underline{\phi}(x)\, du$$

$$\ll \sum_{r=0}^{\infty} \frac{(2\pi)^r X^k}{r!} \int_{\mathfrak{J}(y)} |u - \underline{\alpha} y^k \ell|^r \left| \sum_x{}' x^{kr}\, \underline{\phi}(x)\, e(x^k u) \right| du$$

$$\ll X^k \sum_{r=0}^{\infty} \frac{(2\pi)^r X^{-kr}}{r!} \int_{\mathfrak{J}(y)} \left| \sum_x{}' \underline{\phi}(x)\, x^{kr}\, e(x^k u) \right| du .$$

By Holder's inequality ,

$$|S_\ell(y)|^{2^k} \ll X^{k2^k} \Big(\sum_{r=0}^{\infty} \frac{(2\pi)^{2r}}{r!} \Big)^{2^{k-1}} \sum_{r=0}^{\infty} \frac{X^{-kr2^k}}{r!} \Big(\int_{\mathfrak{J}(y)} \Big| \sum_x{}' \phi(x) x^{kr}\, e(x^k u) \Big| \Big)^{2^k}$$

$$\ll X^k \sum_{r=0}^{\infty} \frac{X^{-rk2^k}}{r!} \mathrm{Ir}$$

by another application of Hölder's inequality. This establishes (49). Our next task is to relate $S(y_m)$ to integrals over $[0,1)$ in a manner similar to Vinogradov (see [16]), and use Lemma 8 to obtain a good estimate for the integrals. We say two intervals $\mathfrak{J}(y_1)$, $\mathfrak{J}(y_2)$ <u>overlap mod 1</u> if there is a real number x and an integer n such that $x \in \mathfrak{J}(y_1)$ and $n + x \in \mathfrak{J}(y_2)$. We will show that not many of the $\mathfrak{J}(y)$ overlap mod 1. Using the periodicity of the integrand in Ir we may then get our required integrals.

Suppose $\mathfrak{J}(y_1)$, $\mathfrak{J}(y_2)$ overlap mod 1, then

$$\underline{\alpha} \ell\, (y_1^k - y_2^k) = h + O(X^{-k})$$

where h is an integer. Thus

$$a\, \ell\, (y_1^k - y_2^k) = h q + O(q X^{-k}) + O(Y^k \ell Q^{-1})$$

$$= hq + O(H)$$

Since $(y_1, q) = (y_2, q) = 1$, there are

$$\ll \left(\frac{\lambda Y_m}{q} + 1\right) q^{\varepsilon}$$

solutions of $y_1^k a \ell \equiv b \pmod q$

in y_1, with $y_m \leq y_1 \leq y_m + t_m$. Thus only

$$\left(1 + \frac{H}{\quad}\right)\left(\frac{\lambda Y_m}{q} + 1\right) q^{\varepsilon}$$

intervals $\mathfrak{J}(y_1)$ can overlap (mod 1) with a given $\mathfrak{J}(y_2)$.

Write $V = \max_v |\underline{\psi}(v)|^{2^k}$, $U = \max_u |\underline{\phi}(u)|^{2^k}$. Then we deduce with one further application of Hölder's inequality that

$$|S(y_m)|^{2^k} \ll Y_m^{2^k} q^{\varepsilon}\left(1 + \frac{H}{\quad}\right)\left(\frac{\lambda}{q} + \frac{1}{y_m}\right) V \sum_{r=0}^{\infty} \frac{X^{k-rk2^k}}{r!} I'_r$$

where $$I'_r = \int_0^1 \Big| \sum_x{}' x^{kr} e(ux^k)\, \underline{\phi}(x) \Big|^{2^k} du$$

$$\ll X^{kr2^k} \left(\frac{N Y_{m-1}}{Y^2}\right)^{2^k - k + \varepsilon} U$$

by Lemma 8. Hence

$$|S(y_m)|^{2^k} \ll F^{2^k} Y_m^{2^k} q^{\varepsilon}\left(1 + \frac{H}{\quad}\right)\left(\frac{\lambda}{q} + \frac{1}{Y_m}\right)\left(\frac{Y_{m-1}}{Y}\right)^{2^k - k} X^{2^k + \varepsilon},$$

Thus

$$\Big| \sum_{y_m \in C_m} S(y_m) \Big|^{2^k}$$

$$\ll F^{2^k} Y_m^{2^k} q^{\varepsilon}\left(1 + \frac{H}{\quad}\right)\left(\frac{\lambda}{q} + \frac{1}{Y_m}\right)\left(\frac{Y_{m-1}}{Y}\right)^{2^k - k} X^{2^k + \varepsilon} \left(\frac{Y}{Y_m}\right)^{2^k}$$

$$\ell y^k = C + mq \ , \quad \text{with} \quad C \equiv b a^{-1} \pmod q$$

$$0 \leq C < q, \quad 0 \leq m \leq L Y^k q^{-1} << L^{1/2} Y^k N^{-k/2}$$

The number of intervals $\mathfrak{J}(y)$ which overlap with a given interval is thus

$$<< (1 + \frac{L^{1/2} Y^k}{N^{k/2}})^2 q^{\varepsilon}$$

$$<< (1 + LY^{2k} N^{-k}) q^{\varepsilon}$$

This is a saving of a factor $(\frac{1}{LY_m} + \frac{Y^{2k}}{N^k Y_m}) q^{\varepsilon}$ over the trivial estimate.

The remainder of the proof follows without difficulty.

Proof of Theorems 3,4,6 & 7

Proof of Theorem 3 As already indicated, we need only estimate sums of type (I) and (II) ((26) and (27)). For $Y \geq N^{1/k}$ we use Lemma 9 ($\ell = L = 1$). This gives an upper bound

$$<< N^{1+\varepsilon/2} (N^{-1/k} + q^{-1})^{2^{-k}} << N^{1-\gamma+\varepsilon/2} \qquad (53)$$

For $N^{1/k} > Y \geq N^{2\gamma}$ we use Lemma 6 with $m = 2$. This also leads to the estimate (53). Finally, for $Y < N^{2\gamma}$ we apply Lemma 6 with $m = 1$ which also gives a suitable bound. As there are only $O(\log N)$ sums of the type (I) and (II) the inequality (4) follows.

Proof of Theorem 7 If $q \geq N^{1 - 1/k}$ the proof follows as above, the $(q^{-1} N^k + \frac{1}{2})^{2^{-k}}$ term coming from Lemma 9 and only being significant for $q > N^{k/2 + \frac{1}{2} - 1/k}$. For $q < N^{1 - 1/k}$ we use Lemma 9 for $Y \geq Q^{2^k}$. For $Q^{2^k} > Y > Q^2$ we use Lemma 6 with $m = 2$. For $Y \leq Q^2$ we use Lemma 6 with $m = 1$.

Proof of Theorem 4 Since α is irrational there are infinitely many different convergents

$$< (F(X\,Y)^{\varepsilon/2+1})^{2^k}(1 + \quad H \quad)(\frac{\lambda}{q} + \frac{1}{Y}) \tag{51}$$

since

$$(\frac{Y_{m-1}}{Y})^{2^k-k}(\frac{1}{Y_m}) \leq \frac{1}{Y}\ .$$

The result of Lemma 9 folows easily from (51) since there are $O(\log N)$ subsums as given in (47) to consider. Slight modifications are necessary in the working for the sum with y range of length Y_1 since the inner sum over x has the form $0 < x < NY^{-1}$, but there are no added difficulties.

LEMMA 10. Suppose we have the hypotheses of Lemma 9, with the added condition that

$$N^{k/2}L^{1/2} << q << N^{k/2}L^{1/2}\ .$$

Then

$$\sum_{\ell=1}^{L} |\sigma_\ell| << (LN)^{1+\varepsilon}\ F(\frac{1}{LY} + \frac{1}{N^{1/2}})^{2^{-k}} \tag{52}$$

where σ_ℓ is the sum on the left hand side of (46).

Proof We shall only outline the necessary modifications to the proof of Lemma 9. By the modulus inequality it suffices to estimate sums of the form (in the notation of (47), (48))

$$\sum_{Y_m \in C_m} \Sigma' |\underline{\psi}(y)| \sum_{\ell=1}^{L} |S_\ell(y)|$$

We proceed as before, relating $S_\ell(y)$ to the same series of integrals. This time however, we are interested in how the intervals are distributed as both y and ℓ vary. We thus require the number of solutions of

$$y^k a\,\ell \equiv b \pmod q$$

for y in a given range of Y_m numbers, $1 \leq \ell \leq L$. We have

to its continued fraction. Let a/q be one such convergent. Pick N so that

$$q = [N^{k/2 + \xi/2 - \varepsilon/2}]$$

and put

$$L = N^{\xi - \varepsilon} .$$

It follows from Lemma 1 of Chapter One that we need only show that

$$\sum_{\ell=1}^{L} \Big| \sum_{p \leq N} (\log p) e(\alpha p^k \ell) \Big| = o(N) \qquad (54)$$

in order to establish a solution of (5) with $N^{\frac{1}{2}} < p \leq N$. Since α is irrational and we pick a sequence of convergents with $q \to \infty$ the result of Theorem 4 follows. As in the case of Theorem 3 we need only consider sums of the type I and II, but we here add an extra summation over ℓ.

Put

$$\rho = k(2k + 2 + (2^k - 1)^{-1})^{-1} .$$

Then

$$\xi + \rho = 2^k \xi , \qquad (55)$$

and

$$k\rho - \xi/2 - k/2 = -2^k\xi, \ \rho - 1 < - 2^k\xi . \qquad (56)$$

We estimate sums of type (I) by Lemma 10 if $N^{\rho} < Y \leq N^{1/2}$. There are $\ll \log N$ such sums, and by (55), (52) we get an upper bound for the total of these sums of

$$\ll (L N)^{\varepsilon/4+1} N^{-(\xi-\varepsilon+\rho)2^{-k}} (\log N)$$

$$= N^{\xi+1-\xi-\varepsilon+\varepsilon/4 - \varepsilon^2/4+\varepsilon 2^{-k} + \xi\varepsilon/4} (\log N)$$

$$= o(N).$$

Assuming, as we may, that ε is sufficiently small. We have used

the fact that $F = O(N^{\varepsilon/8})$ to obtain this result.

For $N^{1/3} \leq Y \leq N^{\rho}$ we estimate sums of type (I) by the case of Lemma 7 with $\phi(x) \not\equiv 1$. It follows from (56) that we get a bound which is $o(N)$ for these sums as well.

We estimate sums of type (II) by the case of Lemma 7 with $\phi(x) \equiv 1$. Here the estimate is

$$N^{1+\varepsilon} L(N^{-k/6} + N^{-2/3})2^{1-k}$$

which is certainly $o(N)$. This establishes (54) and thus completes the proof of Theorem 4.

Proof of Theorem 6 Let α be the leading coefficient of f. Choose N and L as in the proof of Theorem 4, but replacing ξ by σ. Write $Y = N^{2\sigma}$. Let N' be the collection of all numbers of the form $p_1 p_2$ where p_1, p_2 are primes and

$$Y < p_1 \leq 2Y , \quad 4Y^2 < p_1 p_2 \leq N .$$

We note there are $\gg N (\log N)^{-2}$ such numbers. It thus suffices to prove that

$$\sum_{\ell=1}^{L} \Big| \sum_{n \in N'} e(\ell f(n)) \Big| = o(N(\log N)^{-2}) \qquad (57)$$

For $k = 2$ (57) follows from a suitable variant of Lemma 6 (by adding an extra range of summation), taking $m = 2$ and making obvious choices for ϕ and ψ. For $k \geq 3$ (57) is established directly from Lemma 7 (37). This completes the proof of Theorem 6.

We now include a brief demonstration of an improvement upon Graham's result, namely

For irrational α and arbitrary real β there are infinitely many solutions of

$$\| \underline{\alpha} P_2 + \underline{\beta} \| < c\, P_2^{-1/3} (\log P_2)^{4/3} .$$

Here c is a numerical constant which can be evaluated

To prove this, let a/q be a convergent to the continued fraction of $\underline{\alpha}$, $q > 10^6$. Choose X as the largest integer with

$$q > X^2 (\log Xq)^{-2}.$$

Put

$$N = Xq, \qquad L = [c_1 N^{1/3} (\log N)^{-4/3}],$$

where c_1 is a constant < 1. We note that $LX < q$. From lemma 1 of Chapter One it suffices to show that

$$S_L = \sum_{\ell=1}^{L} \Big| \sum_{X^{\frac{1}{2}} < p_1 < X} \; \sum_{X < p_2 \leq q} e(\underline{\alpha} \ell p_1 p_2) \Big| < \frac{M}{6} ,$$

where M is the number of P_2 numbers of the form $p_1 p_2$ occuring in the above sum. Clearly $M \gg N(\log N)^{-2}$. We have, by the modulus inequality,

$$S_L \leq \sum_{m=1}^{LX} h(m) \Big| \sum_{X < p \leq q} e(\underline{\alpha} m p) \Big| .$$

Here $h(m)$ is the number of representations of m as ℓp_1 with $X^{\frac{1}{2}} < p_1 \leq X$. We observe that $h(m) \leq 5$ since $m < X^{5/2}$. As $h(m)$ is non-zero for $\ll LX(\log X)^{-1}$ numbers m, by Cauchy's inequality we have

$$S_L^2 \ll \frac{LX}{(\log X)} \sum_{m=1}^{LX} \Big| \sum_{X < p \leq q} e(\underline{\alpha} m p) \Big|^2$$

We may now use the well known large sieve inequality (see [9]) to estimate the above sum. We get

$$I \ll \max_{u} |\underline{\phi}(u)|^T \int_0^1 \Big| \sum_{A<u\leq A+B} e(\underline{\alpha}_k u^k + \ldots + \underline{\alpha}_1 u) \Big|^T d\underline{\alpha}_1 \ldots d\underline{\alpha}_k \qquad (59)$$

The integral in (59) is the number of solutions in integers x_i, y_i with $A < x_i, y_i \leq A + B$ of the system of equations

$$\sum_{i=1}^{T/2} x_i^s = \sum_{i=1}^{T/2} y_i^s \qquad (s = 1,\ldots k) \qquad (60)$$

We note that the above system is invariant under a translation of all variables by a constant . Hence the integral in (59) is the number of solutions of (60) with $0 < x_i, y_i \leq B$. By Theorem 7 of [7] we find this number to be

$$\ll B^{T-k(k+1)} + \underline{\varepsilon}$$

when $k \leq 10$. For $k = 11$ we get the above result by following Hua's working ($\ell = 40$ in his notation in this case).
For $k \geqslant 12$ we may use Vinogradov's Mean Value Theorem as given by Theorem 4 of [18], which gives an estimate

$$\ll B^{T-k(k+1)} .$$

The proof of the lemma is thus complete.

LEMMA 12 Under all the hypotheses of Lemma 10 with α as the leading coefficient of f we have

$$\sum_{\ell=1}^{L} |\underline{\sigma}_\ell| \ll (LN)^{1+\underline{\varepsilon}} F \left(\frac{1}{LY} + \frac{1}{N^{1/2}} \right)^{1/T} \qquad (61)$$

where T is as given in Lemma 11, and $\underline{\sigma}_\ell$ is the sum of Lemma 10 with f(n) replacing $\underline{\alpha} n^k$.

Proof The proof follows as for Lemmas 9 and 10 with Lemma 11 replacing Lemma 8. The only real difference is that (49) becomes

$$S_L^2 \ll \frac{LX}{\log X} q \sum_{X<p\leq q} 1$$

$$\ll \frac{c_1 q^3}{(\log N)^2}$$

$$\ll \frac{c_1 N^2}{(\log N)^4} .$$

By choosing c_1 sufficiently small the result follows.

We remark that the above method can be adapted to prove a result like Theorem 6 but with the weaker exponent $k((2^k-1)(2k-1) + 2^k)^{-1}$.

4. Proof of Theorem 5 We first require some more lemmas.

LEMMA 11. *Let $\phi(x)$ be an arbitrary function, A and B integers. Then, for $\varepsilon > 0$, we have*

$$I = \int_0^1 \cdots \int_0^1 \left| \sum_{A<u\leq A+B} \phi(u)\, e(\alpha_k u^k + \alpha_{k-1} u^{k-1} + \cdots + \alpha_1 u) \right|^T d\alpha_1 \ldots d\alpha_k \qquad (58)$$

$$\ll B^{T-k(k+1)/2+\varepsilon} \max_{A<u\leq A+B} |\phi(u)|^T$$

Where T is given by the table in the statement of Theorem 5 for $k \leq 11$. For $k \geq 12$ we take

$$T = 4[k^2(\log k + \tfrac{1}{2} \log\log k + 1.3)] .$$

Proof Proceeding as in Lemma 8 we see that

$$|S_\ell(y)|^T \ll \sum_{r_1=0}^{\infty} \cdots \sum_{r_k=0}^{\infty} \frac{X^{-RT} I_R(y) X^{k(k+1)/2}}{r_1!\, r_2! \cdots r_k!}$$

where

$$R = r_1 + 2r_2 + \ldots + k r_k,$$

$$I_R = \int_{\mathfrak{J}_1(y)} \cdots \int_{\mathfrak{J}_k(y)} \Big| \sum_x{}' \phi(x) X^R e(\underline{\alpha}_k x^k + \ldots + \underline{\alpha}_1 x) \Big|^T d\underline{\alpha}_1 \cdots d\underline{\alpha}_k ;$$

and

$$\mathfrak{J}_s(y) = \Big[a_s y^s \ell - \frac{X^{-s}}{2},\ a_s y^s \ell + \frac{X^{-s}}{2} \Big] \qquad (s=1,\ldots k),$$

where a_s is the coefficient of x^s in $f(x)$ (so $a_k = \alpha$).

LEMMA 13 Suppose $k \geq 12$, $N^{k/2} \leq q \leq N^{13k/24}$, $L \leq N$, $(a, q) = 1$, $|\alpha - a/q| \leq (N^k L)^{-1}$, $Y \leq N^{1/3}$. Write, for $\ell \leq L$,

$$S_\ell = \sum_{Y \leq y \leq 2Y}{}' \psi(y) \sum_{x \leq Ny^{-1}}{}' e(\ell f(xy)) .$$

Then

$$S_\ell \ll F N^{1-(3T)^{-1}},$$

Proof Working analogously to Lemmas 5 and 7 we need only estimate

$$S_x(d) = \sum_{n=1}^{x/d} e\Big(\frac{a \ell y^k d^k n^k}{q} + \ell g(ydn) \Big)$$

Here $x \leq NY^{-1}$, g is a polynomial of degree $k-1$ and $(y,q)=1$. Sums with $d > N^{1/4}$ contribute $\ll N^{3/4+\varepsilon}$ to S_ℓ by a trivial estimate, so we may assume $d \leq N^{1/4}$. Similarly we can presume $x/d \geq N^{5/8}$. Let

$$\frac{a \ell y^k d^k}{q} = \frac{b}{q'} \quad \text{with } (b,q') = 1 .$$

References to Chapter Four

1. R.C. Baker, "Small fractional parts of the sequence αn^k", Michigan Math. J. 28 (1981) 223-228.

2. Chen, Jing-Run, "Estimates for trigonometric sums", Chinese Mathematics 1965 vol. 6, 163-167.

3. A. Ghosh, "The distribution of αp^2 modulo one.", Proc. London Math. Soc. (3) 42 (1981) 252-269.

4. S.W. Graham, "Diophantine approximation by almost primes", (Unpublished).

5. G. Harman, "Trigonometric sums over primes I" , Mathematika, 28(1981), 249-254.

6. ————, "Trigonometric sums over primes II", Glasgow Math. J., to appear.

7. L.K. Hua, Additive prime number theory (Amer. Math. Soc. Trans., Vol. 13, Providence, R.I., 1965)

8. L. Kuipers & H. Niederreiter, Uniform distribution of sequences, Wiley-Interscience New York (1974).

9. H.L. Montgomery, "The analytic principle of the large sieve", Bull. Amer. Math. Soc. 84 (1978), 547-567.

10. W.M. Schmidt, Small fractional parts of polynomials, Amer. Math. Soc. Providence, R.I. (1977).

11. R.C. Vaughan, "Mean value theorems in prime number theory", J. London Math. Soc. (2) 10,(1975) 153-162.

12. ————, "Sommes trigonométriques sur les nombres premiers", C.R. Acad. Sci. Paris Serie A 285 (1977) 981-983.

13. ————, "An elementary method in prime number theory",

We have

$$\left(\frac{x}{d}\right)^2 \leq N^2 \leq \frac{N^{k/4}}{L} \leq q' \leq N^{5k/8-k/12} \leq \left(\frac{x}{d}\right)^{k-1}.$$

We are thus able to apply Theorem I of Chapter 6 of [17] to $S_x(d)$ to get the estimate

$$\left(\frac{x}{d}\right) N^{-\delta}$$

where $\delta = 5(24\,k^2 \log(12k(k+1)))^{-1}$. This is more than good enough to prove this lemma. We remark that although we have thrown a lot away in this proof, there is no point in being more precise, since the sticking point in the proof of Theorem 5 is the estimation of sums of type I (i.e.(26)).

Proof of Theorem 5. For $k \leq 11$ the proof follows as for Theorem 4, only using lemma 12 in place of Lemma 10. As we remarked at the end of Lemma 7's proof there is no problem in changing αn^k to $f(n)$.

The value corresponding to ρ in the proof of Theorem 4 is

$$\rho' = (T-1)(2T+(2^{k+1}-1-2k)/k)^{-1}$$

which satisfies

$$\rho'+\tau = T\tau \; ; \; k\rho' - \tau/2 - k/2 = -2^k\tau \; ; \; \rho' - 1 < 2^k\tau .$$

For $k \geq 12$ the proof follows from Lemmas 12 and 13.

CHAPTER FIVE DIOPHANTINE APPROXIMATION BY PRIME NUMBERS

1. Introduction. The main results of this chapter have appeared in a joint paper with R.C. Baker [1b], although Theorem 3 in the present account improves upon the corresponding theorem in that paper for $3 \leq k \leq 6$. When we wrote that paper we were unaware of certain papers by Liu (see his survey paper [6]), many of whose results may be substantially improved by the methods of the present chapter and one such result will be described in section 8. The idea to use the new auxiliary function came from R.C. Baker who also suggested using the method of [14]. The final form of the argument in this chapter is my own however. We prove :

THEOREM 1 *Suppose that* $\lambda_1, \lambda_2, \lambda_3$ *are non-zero real numbers not all of the same sign, that* η *is real, and that* λ_1/λ_2 *is irrational. Let* $\delta > 0$ *be given. Then there are infinitely many ordered triples of primes* p_1, p_2, p_3 *for which*

$$|\eta + \lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3| < (\max p_j)^{-1/6 + \delta}. \tag{1}$$

THEOREM 2 *Given the hypotheses of Theorem 1 and assuming the generalized Riemann hypothesis, there are infinitely many ordered triples of primes* p_1, p_2, p_3 *with*

$$|\eta + \lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3| < (\max p_j)^{-\frac{1}{4}} (\log \max p_j)^4. \tag{2}$$

The basic method we employ can be traced back to Davenport and Heilbronn ([2]). They adapted the Hardy-Littlewood circle method to prove that if $\lambda_1, .., \lambda_s$ are non-zero real numbers, not all of the same sign, and with λ_i/λ_j irrational for some i,j, then for every $\varepsilon > 0$ there are infinitely many solutions in positive integers x_j of the inequality

Acta Arithmetica, 37 (1980), 111-115.

14. I.M. Vinogradov, "A new estimate of a trigonometric sum containing primes", Izv. Akad. Nauk SSSR Ser. Math. 2 (1938) 1-13

15. ————————, "On the estimation of some simplest trigonometric sums involving prime numbers", ibid. 2(1939), 371-395.

16. ————————, "On the estimation of a trigonometric sum over primes," ibid. 12 (1948) 225-248.

17. ————————, The method of trigonometric sums in the theory of numbers (English Trans. 1954, Wiley New York 1954).

18. ————————, Ditto. Russian revised edition, 1971, Moscow.

$$\left| \sum_{j=1}^{s} \lambda_j x_j^k \right| < \varepsilon \qquad (3)$$

provided $s \geq 2^k + 1$. The minimum value of s was subsequently improved for $k \geq 12$ (see [3]) and improved again by Theorem 3 of [11] for $k \geq 5$. Schwarz ([9]) extended the result to show that (3) has infinitely many solutions in primes p_j. By means of a complicated argument A. Baker ([1]) showed that in the case $s = 3$, $k = 1$ the ϵ in (3) may be replaced by $(\log \max p_j)^{-A}$ for any natural number A. This result was extended by Ramachandra ([8]).

A more striking advance was made by R. C. Vaughan ([10] and [11]) who improved the ε to a negative power of $(\max p_j)$ while reducing the necessary size of s for $k \geq 4$ to a value which is $O(k \log k)$. For $s = 3$, $k = 1$ he obtained $(\max p_j)^{-1/10} (\log \max p_j)^{20}$ without the GRH and stated without proof that the $1/10$ could be improved to $1/5$ with the GRH. Our present Theorems 1 and 2 improve these results and we shall indicate how the exponent of $(\max p_j)$ may be improved considerably for $k \geq 2$.

2. Notation and explanation of method. Since λ_1/λ_2 is irrational there are infinitely many different convergents to its continued fraction. Let a/q be one such convergent where q is large in terms

of $\lambda_1, \lambda_2, \lambda_3$ and η. We write, for the proof of Theorem 1,

$$X = q^3 \tag{4}$$

$$\epsilon = X^{\delta - 1/6} \tag{5}$$

$$\mu = 384 |\lambda_1|^{-2} \left(\sum_{j=1}^{3} |\lambda_j| \right)^2 \tag{6}$$

$$P = \mu \epsilon^{-1} \tag{7}$$

$$h = \delta/5 ,$$

$$e(x) = e^{2\pi i x} , \tag{8}$$

$$S_j(x) = \sum_{p \leq X} (\log p)\, e(p x \lambda_j) \tag{9}$$

$$V(x) = \min(|S_1(x)|, |S_2(x)|) \tag{10}$$

$$I(x) = \int_0^X e(xy)\,dy ,$$

$$G(x) = \prod_{j=1}^{3} I(\lambda_j x) \tag{11}$$

$$F(x) = \prod_{j=1}^{3} S_j(x) \tag{12}$$

$$\tau = X^{-4/5} (\log X)^{-1} . \tag{13}$$

Constants implied by $<<$ shall depend only on $\lambda_1, \lambda_2, \lambda_3$ and η. The following lemma converts the problem of solving inequalities of the form (1), (3) into a question of estimating exponential sums and integrals. We use this result in place of the more familiar Lemma 4 of [2] merely to simplify certain parts of the argument; it is not a necessary ingredient in improving Vaughan's work.

LEMMA 1 For any $g > 0$ there is a continuous function $A(x)$ in $L'(R)$ such that

$$A(x) \leqq \chi_{[-1,1]}(x) . \tag{14}$$

While, if we write

$$\hat{A}(t) = \int_{-\infty}^{\infty} A(y)\, e(-ty)dy , \tag{15}$$

then $\hat{A}(t) = 0$ for $|t| \geqq g$ (16)

Also

$$\int_{-\infty}^{\infty} \left(\chi_{[-1,1]}(x) - A(x)\right) dx = g^{-1} . \tag{17}$$

Proof See p.559 of [7]. Henceforth $A(x)$ shall denote the function given by Lemma 1 with $g = \mu$.

COROLLARY. Let $N(X)$ denote the number of solutions of the inequality

$$|\eta + \lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3| < \varepsilon$$

in primes $p_1, p_2, p_3 \leqq X$. Then

$$\varepsilon^{-1}(\log X)^3 N(X) \geqq \int_{-\infty}^{\infty} e(x\eta)F(x)\hat{A}(\varepsilon x)dx . \tag{18}$$

Proof From (10) and (12)

$$\int_{-\infty}^{\infty} e(x\eta)F(x)\hat{A}(\varepsilon x)dx = \sum_{p_1,p_2,p_3 \leqq X} \prod_{i=1}^{3} (\log p_i) \int_{-\infty}^{\infty} e\Big(x\big(\eta + \sum_{j=1}^{3} \lambda_j p_j\big)\Big)\hat{A}(\varepsilon x)dx \tag{19}$$

The integral in (19) may be estimated by a well known theorem on the inversion of a Fourier integral (both A and $\hat{A}$ are in $L'(R)$, of course). The integral is simply

3. Region one. Here $|x| \leq \tau$, and this part of the integral forms the main positive contribution to the integral.

LEMMA 2 We have

$$\int_{-\tau}^{\tau} |F(x) - G(x)|\,|\hat{A}(\varepsilon x)|\,dx \ll X^2 (\log X)^{-1} . \tag{20}$$

Proof It is established in [10], Lemma 9, that

$$\int_{-\tau}^{\tau} |F(x) - G(x)|\,dx \ll X^2 (\log X)^{-1} .$$

From Lemma 1 $\hat{A}(\varepsilon x) \ll 1$, so (20) follows.

LEMMA 3 We have

$$\int_{-\infty}^{\infty} e(x\eta) G(x) \hat{A}(\varepsilon x)\,dx \gg X^2 . \tag{21}$$

Proof We write $D(y) = \chi_{[-1,1]}(y) - A(y)$ and put

$$Q^* = \int_0^X \int_0^X \int_0^X \max(0, \varepsilon - |\eta + \sum_{j=1}^{3} \lambda_j y_j|)\,dy_1\,dy_2\,dy_3 .$$

In the proof of Lemma 10 of [10] it is shown that

$$Q^* > \frac{3}{|\lambda_1|\mu}\,\varepsilon^2 X^2 . \tag{22}$$

(That part of Vaughan's argument does not depend on the size of ε).

By an easily justified interchange in the order of integration,

$$\int_{-\infty}^{\infty} e(x\eta) G(x) \hat{A}(\varepsilon x)\,dx = \int_0^X \int_0^X \int_0^X e(x(\eta + \sum_{j=1}^{3} \lambda_j y_j)) \hat{A}(\varepsilon x)\,dx\,dy_1 dy_2 dy_3$$

$$= \int_0^X \int_0^X \int_0^X \frac{1}{\varepsilon} A\left(\frac{\eta + \lambda_1 y_1 + \lambda_2 y_2 + \lambda_3 y_3}{\varepsilon}\right) dy_1\,dy_2\,dy_3$$

$$\varepsilon^{-1} A((\eta + \sum_{j=1}^{3} p_j\lambda_j)\varepsilon^{-1}).$$

From this and (1) we see that (18) follows.

We observe that the integral in (18) is really only over a finite range (by (16)) of length P, i.e. $\ll \varepsilon^{-1}$. The normal procedure is to obtain an infinite integral, whose range of integration is split into three sections, traditionally named (with variations): the neighbourhood of the origin; the intermediate region; the trivial region. In Vaughan's work this corresponds to $|x| \leqq \tau$, $\tau < |x| \leqq \varepsilon^{-2}$, $\varepsilon^{-2} < |x|$, respectively. We shall split our range of integration in three as well, but our regions are: $|x| \leqq \tau$; $\tau < |x| \leqq 1$; $1 < |x| \leqq P$. We shall draw heavily on Vaughan's analysis for the first region. It is possible to improve Vaughan's work to reduce our present approach to two regions: $|x| \leqq X^{-\delta}$, $X^{-\delta} < |x| \leqq P$. However, the argument is more complicated and the idea of using three regions enables us to further improve the exponent of $(\max p_j)$ when $k \geqq 7$. The reason for this is that the maximum permissible value of τ may not be improved beyond $X^{-k+1-\delta}$, whereas we would like $|x|$ to exceed $X^{-k/2}$ throughout the "intermediate region". (see section 6).

The second region with $\tau < |x| \leqq 1$ is the easiest to estimate. For k^{th} powers of primes any value of $\tau > X^{-k+\delta}$ will suffice. By modifying the argument in [11] we could take $\tau = X^{-k+\frac{1}{2}-\delta}$. The third region is the "sticking point" as regards improving the exponent. Theorems 1 and 2 shall be proved by showing that the integral in (18) is $\gg X^2$. The analysis in sections 3 and 4 is little affected by altering the relative sizes of X, q and ε, which we do to prove Theorem 2.

$$= \int_0^X\int_0^X\int_0^X \frac{1}{\varepsilon}\left(X_{[-1,1]}\left(\frac{\eta+\lambda_1 y_1+\lambda_2 y_2+\lambda_3 y_3}{\varepsilon}\right) - D\left(\frac{\eta+\lambda_1 y_1+\lambda_2 y_2+\lambda_3 y_3}{\varepsilon}\right)\right) dy_1 dy_2 dy_3$$

$$\geq Q^* \varepsilon^{-2} - \int_0^X\int_0^X\int_0^X \varepsilon^{-1}\, D(\varepsilon^{-1}(\eta + \sum_{j=1}^{3} \lambda_j y_j))\, dy_1 dy_2 dy_3$$

$$\geq Q^* \varepsilon^{-2} - \int_0^X\int_0^X\int_{0-\infty}^{\infty} \varepsilon^{-1}\, D(\varepsilon^{-1}(\eta + \sum_{j=1}^{3} \lambda_j y_j))\, dy_1 dy_2 dy_3 \quad \text{(since } D(y) \geq 0\text{)}$$

$$> \frac{3X^2}{|\lambda_1|\mu} - X^2 \int_{-\infty}^{\infty} D(\lambda_1 y)\, dy \quad \text{by (22) and a trivial bound}$$

$$\geq \frac{2X^2}{|\lambda_1|\mu} \quad \text{by (17)}$$

$$>> X^2 \quad \text{as required.}$$

LEMMA 4 We have

$$\int_{-\tau}^{\tau} e(x\eta)\, G(x)\, \hat{A}(\varepsilon x)\, dx >> X^2 . \tag{23}$$

Proof Since $\hat{A}(\varepsilon x) << 1$ and we have the inequality (21), it suffices to show that

$$\int_{|x|>\tau} |G(x)|\, dx = o(X^2) . \tag{24}$$

We have

$$I(x) = \int_0^X e(xy)\, dy << \min(X, x^{-1}) .$$

Thus $$\int_{|x|>\tau} |G(x)|\, dx << \int_{\tau}^{\infty} x^{-3}\, dx$$

$$<< \tau^{-2}$$

$$= X^{8/5} (\log X)^2 .$$

Thus (24) is established and the proof complete.

LEMMA 5 We have

$$\int_{-\tau}^{\tau} e(\eta x) F(x) \hat{A}(\varepsilon x)\, dx >> X^2 .$$

Proof This is immediate from (20) and (23).

If we are dealing with the problem involving k^{th} powers of primes the sizes of ε and τ will be different, as already remarked, and the lower bound of Lemma 5 will become

$$\int_{-\tau}^{\tau} F_k(x) \hat{A}(\varepsilon x)\, dx >> X^{s-k}$$

where

$$F_k(x) = \prod_{j=1}^{s} \sum_{p_j \leq X} e(x p_j^k) (\log p_j).$$

4. Region two. Here $\tau < |x| \leq 1$.

LEMMA 6 Suppose $|r\alpha - b| < r^{-1}$, $(b,r) = 1$. Then

$$\sum_{p \leq N} (\log p)\, e(p\alpha) << (\log N)^{7/2} (N^{4/5} + Nq^{-\frac{1}{2}} + N^{\frac{1}{2}} q^{\frac{1}{2}}) . \qquad (25)$$

Proof See [12].

LEMMA 7 For $\tau < |x| \leq 1$ we have

$$V(x) << X (\log X)^{-2} . \qquad (26)$$

Proof We first remark that it is possible to improve (26) considerably, but this is unnecessary here. We observe that (26) is true for k^{th} powers of primes and any $\tau > X^{-k+\delta}$ by using Theorem 1 of [4] in place of Lemma 6 here. For a given x, we may choose q_1, q_2, a_1, a_2 such that

$$|\lambda_j x - a_j/q_j| \leq X^{-1} (\log X)^{20} q_j^{-1}$$

with $(a_j,q_j) = 1$ and $1 \leq q_j \leq X (\log X)^{-20}$. As $\tau = X^{-4/5} (\log X)^{-1}$ we see that $a_1 a_2 \neq 0$. Now suppose that both q_1 and q_2 are less than $(\log X)^{20}$. We have

$$a_2 q_1 \frac{\lambda_1}{\lambda_2} - a_1 q_2 = \frac{a_2/q_2}{\lambda_2 x} q_1 q_2 \left(\lambda_1 x - \frac{a_1}{q_1}\right) - \frac{a_1/q_1}{\lambda_2 x} q_1 q_2 \left(\lambda_2 x - \frac{a_2}{q_2}\right)$$

$$\ll X^{-1} (\log X)^{40} .$$

Since $q = X^{1/3}$ we have

$$\left| a_2 q_1 \frac{\lambda_1}{\lambda_2} - a_1 q_2 \right| = o(q^{-1}) . \tag{27}$$

But $|a_2 q_1| \leq (\log X)^{40} = o(q)$. (28)

We note that (27), (28) contradict the definition of q as the denominator of a convergent to λ_1/λ_2, for q sufficiently large (see Lemma 9(ii)). Thus one of q_1, q_2 is greater than $(\log X)^{20}$. This with (25) establishes (26).

LEMMA 8 We have

$$\int_{\tau < |x| \leq 1} |F(x) \hat{A}(\varepsilon x)| \, dx \ll X^2 (\log X)^{-1} . \tag{29}$$

Proof We have

$$\int_{\tau < |x| \leq 1} |F(x)\, \hat{A}(\varepsilon x)|\, dx \ll \int_{\tau < |x| \leq 1} |F(x)|\, dx$$

$$\leq \max_{|x| \in [\tau, 1]} V(x) \sum_{j=1}^{3} \int_0^1 |S_j(x)|^2\, dx$$

$$\ll X^2 (\log X)^{-1} .$$

Here we have used (26) and

$$\int_0^1 |S_j(x)|^2\, dx \ll \int_0^1 \Big| \sum_{p \leq X} \log p\, e(xp) \Big|^2 dx$$

$$\ll X \log X \qquad (30)$$

by Chebychev's upper bound.

Lemma 8 demonstrates that the contribution from region 2 is of a smaller order of magnitude than that from region 1. For k^{th} powers of primes the right hand side of (29) becomes

$$X^{s-k} (\log X)^{-1}$$

for $s \geq s_0(k)$. Here $s_0(2) = 5$, $s_0(3) = 9$ and, for $k \geq 4$, $s_0(k)$ is Vaughan's $\mathfrak{D}(k)$ of Corollaries 2.1 and 2.2 of ([11]). For example, $s_0(4) = 15$, $s_0(10) = 123$. To establish (29) for $k \geq 4$ we have to estimate an integral (cf. (5.29) of [11]) of the form

$$\mathcal{J} = \int_0^1 |S_j(x)|^{2\ell} |H(x)|^2\, |\hat{A}(\varepsilon x)| dx .$$

Here $H(x)$ is a certain exponential sum (Vaughan's $F_t(x)$). We note that for $0 \leq x \leq 1$

$$\hat{A}(\varepsilon x) << 1 << \left(\frac{\sin \pi x/2}{\pi x}\right)^2 .$$

Thus

$$\mathfrak{f} << \int_{-\infty}^{\infty} |S_j(x)|^{2\ell} |H(x)|^2 \left(\frac{\sin \pi x/2}{\pi x}\right)^2 dx .$$

The above integral represents the number of solutions of a certain inequality and so is bounded above by the number of solutions with p_j replaced by n_j (i.e. summing over all n in $S_j(x)$, not just primes). We may then use Theorem 1 of [11] with $\varepsilon = 1/2$ to conclude that

$$\mathfrak{f} << X^{s-1-k+\delta}$$

essentially. This is the desired form of inequality to replace (30) in the case $k \geq 4$.

5. Region three. As we have previously remarked, this is the crucial region, and here we employ an argument given by G. L. Watson in section 10 of [14]. This enables us to improve the method we used in Lemma 7 of section 4 which closely followed Lemma 11 of [10] and Lemma 13 of [3].

LEMMA 9 Let b/r be any convergent to the continued fraction for α. Then the inequality

$$|\alpha - \phi/\nu| < (4r\nu)^{-1}$$

in which ϕ, ν denote integers, not necessarily coprime and ν is positive, is not soluble

$$|\lambda_1 x q_1 - a_1| < X^{-1+h} (X/Z)^2 , \qquad (34)$$

$(q_1, a_1) = 1$ and $q_1 \leq X^h (X/Z)^2$.

We divide $M(Z)$ into disjoint subsets $M(Z, Q_1, Q_2)$ such that

$$Q_1 < q_1 \leq 2Q_1 , \qquad Q_2 < q_2 \leq 2Q_2$$

for $x \in M(Z, Q_1, Q_2)$. From (34) it can be seen that $M(Z, Q_1, Q_2)$ is contained in intervals of length $< 2\lambda_1^{-1} Q_1^{-1} X^{-1+h} (X/Z)^2$. We now show that there are not very many of these. Working as in Lemma 7 we find that

$$\left| a_2 q_1 \frac{\lambda_1}{\lambda_2} - a_1 q_2 \right| < X^{-1/3-h} = o(q^{-1}).$$

We have $a_2 q_1 \leq q_1 q_2 P << Q_1 Q_2 P$.

So, by Lemma 9(iii) $a_2 q_1$ can take on only

$$Q_1 Q_2 P q^{-1}$$

values. By (i) of Lemma 9 each value of q_1 defines precisely one value of a_1. Since the number of divisors of $a_2 q_1$ is $<< X^h$ by a well known estimate, $M(Z, Q_1, Q_2)$ is contained in

$$<< Q_1 Q_2 P q^{-1} X^h$$

intervals (34). Now $|S_2(x)|^2 << X^{2+h} Q_2^{-1}$ by (25), so

$$\int_{M(Z,Q_1,Q_2)} |S_1(x) S_2(x)|^2 dx << (Q_1 Q_2 P q^{-1} X^h)(Q_1^{-1} X^{1+h} Z^{-2}) Z^2 X^{2+h} Q_2^{-1}$$

$$= P X^{3+3h} q^{-1}$$

$$<< \varepsilon X^{3-\delta-h} \quad \text{by (4), (5), (7).}$$

(i) for two different ϕ and the same ν,

(ii) for any $\nu < r$,

(iii) for any two different ν differing by less than r.

Proof This is Lemma 2 of [14].

The following lemma is the most significant step in improving Vaughan's result in [10] (it is quite easy to improve his 1/10 to 1/9, but a result like the following is needed to make any saving over 1/9).

LEMMA 10 There is a set of numbers $M \subset [1, P]$ such that

(i) for $|x| \in [1, P)$, $|x| \notin M$ we have

$$V(x) \leq X^{1-\delta/2} \varepsilon \tag{31}$$

(ii) $$\int_{|x| \in M} |S_1(x)S_2(x)|^2 \, dx \ll X^{3-\delta} \varepsilon . \tag{32}$$

Proof We define M to be the set of all $x \in [1,P]$ for which (31) is untrue. We may also suppose $|S_1(x)| \geq |S_2(x)|$ since M can be split into two subsets and the proof for $|S_1(x)| < |S_2(x)|$ will follow analogously. We now divide M into $\ll \log X$ disjoint subsets $M(Z)$ such that

$$Z < |S_1(x)| \leq 2Z \tag{33}$$

for $x \in M(Z)$. For each $x \in M(Z)$ we pick a_2, q_2 so that $q_2 \leq X^{2/3}$, $|\lambda_2 x q_2 - a_2| < X^{-2/3}$, $(a_2, q_2) = 1$. By the definition of M, $|S_2(x)| > X^{5/6 + \delta/2}$ so, by (25), $q_2 < X^{1/3 - h}$. Also, by (25) and (33) there is a pair q_1, a_1 with

The proof is completed upon noting that there are $\ll (\log X)^3 \ll X^h$ subsets $M(Z, Q_1, Q_2)$.

LEMMA 11 We have

$$\int_{|x|>1} |F(x)\,\hat{A}(\varepsilon x)|\,dx \ll X^{2-h}. \tag{35}$$

Proof By (31),

$$\int_{\substack{|x|>1\\ |x|\notin M}} |F(x)\,\hat{A}(\varepsilon x)|\,dx \ll X^{1-\delta/2}\varepsilon \sum_{j=1}^{3} \int_0^P |S_j(x)|^2\,dx$$

$$\ll X^{1-\delta/2}\varepsilon\, P \int_0^1 \Big| \sum_{p\le X} e(xp)(\log p)\Big|^2 dx$$

$$\ll X^{2-h}.$$

Also

$$\int_{|x|\,\varepsilon\, M} |F(x)|\,dx \le \left(\int_{x\,\varepsilon\, M} |S_1(x)S_2(x)|^2\,dx \int_0^P |S_3(x)|^2\,dx\right)^{\frac{1}{2}}$$

$$\ll (X^{3-\delta}\,\varepsilon X\, P \log X)^{\frac{1}{2}}$$

$$\ll X^{2-h}.$$

This completes the proof of (35).

6. Proof of Theorem 1 and other results. By Lemmas 5, 8 and 11,

$$\int_{-\infty}^{\infty} e(x\eta)\,F(x)\,\hat{A}(\varepsilon x)\,dx \gg X^2.$$

Thus, from (18), the number of solutions of (1) is

$$\gg \varepsilon X^2 (\log X)^{-3}$$

$$\gg X.$$

Since X tends to infinity with q, this completes the proof.

To prove results for k-th powers of primes we take q as before and define X, Y, W, ε, by the following table :

k	X	ε	Y	W
2	q	$X^{-\frac{1}{8}} + \delta$	$X^{\frac{1}{2}} - 8h$	$X^{1\frac{1}{2}} - 4h$
3	$q^{\frac{7}{8}}$	$X^{-1/28} + \delta$	$X^{4/7} - 8h$	$X^{12/7} - 4h$
≥ 4	$q^{2/(k-1)}$	$X^{-(k2^k)^{-1}} + \delta$	$X^{1} - 1/k - 8h$	$X^{(k+1)/2 - 4h - 1/k}$

For $k \geq 11$ we may take $\varepsilon = X^{-(25k^2 \log k)^{-1}} + \delta$.

The analogue of Lemma 10 for k-th powers of primes is :

LEMMA 10 B Let M be the set of x in $[1,P)$ such that

$$\min (S_1(x), S_2(x)) \ll \varepsilon X^{1 - 2h} \quad \text{for } x \notin M$$

Then

1) For $2 \leq k \leq 4$ we have

$$\int_{x \in M} |S_1(x) \ldots S_s(x)| \, |\hat{A}(\varepsilon x)| \, dx \ll X^{1-2h} \int_{-\infty}^{\infty} K_{\frac{1}{2}}(x) \, (F(x)^2 + G(x)^2) \, dx.$$

Here $F(x)$ and $G(x)$ are any two disjoint products of $(s-1)/2$ of the moduli of the sums $S_2(x), \ldots, S_s(x)$.

2) For $k \geq 5$ M is empty, assuming q is sufficiently large.

Proof We pick q_1, q_2, a_1, a_2 as in Lemma 10 but replacing $X^{2/3}$ by W. By Theorem 7 of Chapter 4* we have $q_j < Y$ $(j=1,2)$. We define $M(Z, Q_1, Q_2)$ as in Lemma 10. By the argument of that lemma $M(Z, Q_1, Q_2)$ is contained in $\ll Q_1 Q_2 q^{-1} \varepsilon^{-1} X^h$ intervals of length < 1. If $k \geq 5$ there are therefore no such intervals, assuming q is sufficiently large. Now we note that, for any $A' > 0$,

---

* for $k = 2$ use Theorem 1.

$$\int_{A'}^{A'+1} |S_2(x) \ldots S_s(x)| \; |\hat{A}(\varepsilon x)| \, dx \ll \int_{A'}^{A'+1} (F(x)^2 + G(x)^2) dx$$

$$\ll \int_{-\infty}^{\infty} (F(x)^2 + G(x)^2) K_{\frac{1}{2}}(x - A') dx \ll \int_{-\infty}^{\infty} (F(x)^2 + G(x)^2) \, K_{\frac{1}{2}}(x) \, dx.$$

It thus remains to show that the number of intervals in which $M(Z, Q_1, Q_2)$ is contained is $\ll X^{1-3h} Z^{-1}$.

A). $k = 2$. By Theorem 1 of Chapter Four we have $Z < Q_1^{-\frac{1}{4}} X^{1+h}$ so

$$Q_1 Q_2 \, q^{-1} X^h \varepsilon^{-1} Z \ll X^{2h} Q_1^{\frac{3}{4}} Q_2 X^{\frac{1}{8}} - \delta \ll Y^{7/4} X^{\frac{1}{8}+2h-\delta} \ll X^{1-3h}$$

as required.

B). $k = 3$. This time we use Theorem 7 of the previous chapter to find that

$$Z < Q_1^{-1/16} X^{1+h}$$

Hence

$$Q_1 Q_2 \, q^{-1} X^h \varepsilon^{-1} Z \ll X^{2h - 3/28 - \delta} Y^{31/16} \ll X^{1-3h}$$

as required.

C). $k = 4$. Here we note that $Z < X^{1+h} Q_1^{-1/48}$, and the proof may be completed as above.

The following Theorem follows easily from Lemma 10b, the results already mentioned in this chapter, and the working in [11] :

THEOREM 3 Define $s_0(k)$ by

k	2	3	4	5	6	7	8	9	10
$s_0(k)$	5	9	15	25	37	55	75	97	123

and, for $k \geq 10$

$$s_0(k) = 2k + 7 + 2 \, (-\log 2R + \log (1 - 2/k))/(-\log(1 - 1/k))$$

where $R = 2^{1-k}$ $(k \leq 12)$, $= (2k^2(2 \log k + \log\log k + 3))^{-1}$ $(k > 12)$.

Let s be an integer $\geq s_0(k)$ and suppose that $\lambda_1, \lambda_2, \ldots, \lambda_s$ are non-

zero real numbers not all of the same sign, that η is real, and λ_1/λ_2 is irrational. Let $\delta > 0$ be given. Then there are infinitely many ordered s-tuples of primes $p_1,\dots,p_s$ with

$$\left| \eta + \sum_{j=1}^{s} \lambda_j p_j^k \right| < (\max p_j)^{-\gamma + \delta}.$$

Here

$$\begin{aligned} \gamma &= \tfrac{1}{8} && \text{if } k = 2 \\ &= 1/28 && \text{if } k = 3 \\ &= (k2^k)^{-1} && \text{if } 10 \geqq k \geqq 4 \\ &= (25k^2 \log k)^{-1} && \text{if } k \geqq 11. \end{aligned}$$

The value given by Vaughan for γ is the much weaker $(5.4^{k+1}(k+1))^{-1}$. To prove the result for $k \geqslant 11$, it is necessary to use the result of [13] in place of Theorem 7 of Chapter 4.

7. Proof of Theorem 2. We now write

$$X = q^2, \qquad \varepsilon = X^{-\frac{1}{4}} (\log X)^4,$$

The proof for regions one and two may be completed as before. The following lemma, dependent on the Generalized R iemann Hypothesis is the only significant change in the proof of Theorem 2.

LEMMA 12 Suppose $\beta = \alpha - a/q$, $(a,q) = 1$, $|\beta| \leq N^{-\frac{1}{2}}$. Then, on the GRH, we have

$$\sum_{n=1}^{N} \Lambda(n)e(\alpha n) << \left\{ \frac{|\mu(q)|}{(\log N)q} \min(N, |\beta|^{-1}) + N^{\frac{1}{2}} q^{\frac{1}{2}} \left(1 + \frac{N^{\frac{1}{2}} \beta^{\frac{1}{2}}}{(\log N)^{\frac{1}{2}}} \right) \right\} (\log N)^2 . \quad (36)$$

Proof We may suppose that $q \leq N$. Let χ denote a Dirichlet character modulo q. We first note the well known results on Gauss sums

$$\left.\begin{aligned} \tau(\bar{\chi}) = \sum_{n=1}^{q} \bar{\chi}(n) e(n/q) &= \mu(q) \quad \text{if } \chi = \chi_0, \text{ the principal character} \\ &<< q^{\frac{1}{2}} \quad \text{otherwise.} \end{aligned}\right\} \quad (37)$$

Write

$$\sigma = \sum_{\substack{n=1 \\ (n,q)=1}}^{N} \Lambda(n) e(\alpha n) .$$

Clearly

$$\sum_{n=1}^{N} \Lambda(n) e(\alpha n) - \sigma << \log q . \quad (38)$$

We may thus work with σ in order to prove (36). We have

$$\sigma = \frac{1}{\phi(q)} \sum_{\chi} \chi(a) \tau(\bar{\chi}) \sum_{n=1}^{N} \Lambda(n) \chi(n) e(n\beta) . \quad (39)$$

formula (24) of [10].) From (41) and (42) we get

$$\sum_{n=1}^{N} \Lambda(n)\chi(n)e(n\beta) = O(N^{\frac{1}{4}}(\log N)^{\frac{3}{2}}) + O(N^{\frac{5}{4}}\beta(\log N)^{\frac{3}{2}}) - \Sigma' \mathcal{J}_\rho . \quad (43)$$

Here

$$\mathcal{J}_\rho = \int_1^N u^{\rho-1} e(u\beta)\,du = \int_1^N u^{-\frac{1}{2}} e\left(u\beta + \frac{\gamma \log u}{2\pi}\right) du ,$$

if $\gamma = \mathcal{J} m\rho$. We may estimate $\mathcal{J}_\rho$ by Van der Corput's well known methods using the size of the first and second derivatives of $u\beta + (\gamma \log u)/2\pi$. We find that

$$\mathcal{J}_\rho \ll \min\left(\max_{u\leq N} \frac{u^{\frac{1}{2}}}{|2\pi u\beta + \gamma|}\ ,\ \max_{u\leq N} \frac{u^{\frac{1}{2}}}{|\gamma|^{\frac{1}{2}}}\right).$$

Thus $\mathcal{J}_\rho \ll N^{\frac{1}{2}}|\gamma|^{-\frac{1}{2}}$ for $|\gamma| < 4\pi N\beta$

$\ll N^{\frac{1}{2}}|\gamma|^{-1}$ for $|\gamma| > 4\pi N\beta$.

Hence

$$\Sigma' \mathcal{J}_\rho \ll N^{\frac{1}{2}}(\log N)^2 + N|\beta|^{\frac{1}{2}}(\log N). \quad (44)$$

Combining (43), (44) yields

$$\sum_{n=1}^{N} \Lambda(n)\chi(n)e(n\beta) = O(N^{\frac{1}{2}}(\log N)^2 + N|\beta|^{\frac{1}{2}}(\log N)^{\frac{3}{2}}). \quad (45)$$

(We here use $\beta \leq N^{-\frac{1}{2}}$; by working a little more carefully we could dispense with this hypothesis, but it does not affect our results.)

For $\chi = \chi_0$ an extra term Y is necessary on the right of (40)

Now let χ be any of the non-principal characters in (39). For any real number $Y > 1$, we have the well known estimate

$$\sum_{n \leq Y} \Lambda(n)\chi(n) = -\Sigma' \frac{Y^\rho}{\rho} + O(YT^{-1}\log^2 Yq + Y^{\frac{1}{4}}\log Y) \tag{40}$$

$$= -\Sigma' \frac{Y^\rho}{\rho} + O(N^{\frac{1}{4}}(\log N)^{3/2}) \tag{41}$$

Here Σ' indicates summation over all zeros of $L(s,\chi)$ (on $s = \frac{1}{2}$ since we assume the GRH), with $|\text{Im } \rho| \leq T$. To get (41) we have put $T = N^{\frac{3}{4}}(\log N)^{\frac{1}{2}}$ and presumed that $Y \leq N$.

Now suppose f and g are functions possessing continuous derivatives and that

$$\sum_{M \leq n \leq u} c_n = g(u) + h(u)$$

Then, by partial summation/integration we find that

$$\sum_{M \leq n \leq L} c_n f(n) = f(L)h(L) + \int_M^L g'(u)f(u)du + f(M)g(M) - \int_M^L h(u)f'(u)du. \tag{42}$$

(The present author believes that the formula (42) is clearer than the one used by Vaughan who needs to integrate by parts after application of the

and (41). This gives

$$\sum_{n=1}^{N} \Lambda(n)\chi_0(n)\, e(n\beta) = \int_1^N e(u\beta)du + O(N^{\frac{1}{2}}(\log N)^2 + N|\beta|^{\frac{1}{2}}(\log N)^{\frac{3}{2}})$$

$$\ll \min(N, |\beta|^{-1}) + O(N^{\frac{1}{2}}(\log N)^2 + N|\beta|^{\frac{1}{2}}(\log N)^{\frac{3}{2}}). \quad (46)$$

Combining (37), (39), (45), (46) gives

$$\sigma \ll \frac{|\mu(q)|}{\phi(q)} \min(N, |\beta|^{-1}) + N^{\frac{1}{2}} (\log N)^2 q^{\frac{1}{2}} + N|\beta|^{\frac{1}{2}} q^{\frac{1}{2}} (\log N)^{\frac{3}{2}} . \quad (47)$$

The proof of Lemma 12 is completed by observing that (36) follows from (38) and (47) together with the obvious inequality $\phi(q) \gg q (\log q)^{-1}$.

LEMMA 13 On the GRH there is a set of numbers $M \subset [1,P]$ such that, for $1 \leq x \leq P$,

(i) for $x \notin M$, $V(x) \leq X^{\frac{3}{4}} (\log X)^{\frac{5}{2}}$ (48)

(ii) $$\int_M |S_1(x)\, S_2(x)|^2 \, dx \ll X^{\frac{8}{3}} .$$ (49)

Proof We work as in Lemma 10, but pick q_2, a_2 with $|\lambda_2 q_2 x - a_2| < X^{-\frac{1}{2}}$, $q_2 \leq X^{\frac{1}{2}}$. By (36) and (48) $q_2 \ll X^{\frac{1}{4}} (\log X)^{-\frac{3}{2}}$ and $|\lambda_2 q_2 - a_2| < X^{-\frac{3}{4}} \times$ $\times (\log X)^{-\frac{3}{2}}$. Also, by (36) we may find a_1, q_1 with

$$|\lambda_1 q_1 x - a_1| < Z^{-1} (\log X),$$

$$1 \leq q_1 < X Z^{-1} (\log X), \quad (a_1, q_1) = 1 .$$

Thus

$$\left| a_2 q_1 \frac{\lambda_1}{\lambda_2} - a_1 q_2 \right| << X^{-\frac{1}{2}} (\log X)^{-1} = o(q^{-1}) . \qquad (50)$$

From (50) we can split M into $<<(\log X)^3$ subsets $M(Z, Q_1, Q_2)$ each of measure

$$<< Q_2 P q^{-1} X^{1/10} Z^{-1} .$$

(We here use the trivial inequality that a number less than X has $<< X^{1/11}$ divisors.) Also

$$Q_1 Q_2 P >> q . \qquad (51)$$

We have, for $x \in M(Z, Q_1, Q_2)$,

$$|S_1(x) S_2(x)|^2 << Q_2^{-2} Q_1^{-1} Z X^3 (\log X)^3 .$$

Thus

$$\int_{M(Z,Q_1,Q_2)} |S_1(x) S_2(x)|^2 \, dx << P X^{3+1/10} q^{-1} (Q_1 Q_2)^{-1} (\log X)^3$$

$$<< P^2 X^{3+1/10} q^{-2} (\log X)^3 \text{ by (51)}$$

$$<< X^{8/3} (\log X)^{-3} .$$

Hence

$$\int_M |S_1(x) S_2(x)|^2 \, dx << X^{8/3}$$

as required.

The proof of Theorem 2 may now be completed easily.

8. Results for mixed powers. The following result may be demonstrated easily using the methods of this chapter and Theorem 1 from the previous one.

THEOREM 4 *Let* $\lambda_1, \lambda_2, \ldots, \lambda_s$ *be non-zero real numbers, not all of the same sign with* λ_1/λ_2 *irrational. Suppose* $k_1, \ldots, k_s$ *are positive integers such that*

$$\sum_{j=1}^{s} 2^{-k_j} \geq 1 + 2^{-t}$$

where $t = \min k_j$. *Let* $f_j(x)$ *be polynomials of degree* k_j *with integer coefficients, the leading one being positive. Let* η *be an arbitrary real number. Then there are infinitely many ordered s-tuples of primes with*

$$\left| \eta + \sum_{j=1}^{s} \lambda_j f(p_j) \right| < (\max p_j^{k_j}) - E(k_1,k_2) + \delta$$

where

$$E(k_1,k_2) = \min \left(\frac{2^{1-2k_1}}{k_1}, \frac{2^{1-2k_2}}{k_2} \right) \quad \text{for } \max(k_1,k_2) > 1$$

$$= 1/6 \quad \text{if } k_1 = k_2 = 1,$$

and $\delta > 0$.

Undoubtedly better bounds for the number of variables required may be found by adapting Vaughan's argument in [11]. Also one can improve the 2^{1-2k_j} terms for large k, or for k greater than two if f is a monomial. Theorem 4 improves on the work of Liu because of the new estimates for trigonometric sums over primes (Chapter 4 here) and also because of the refinements we have made to the traditional (Davenport - Heilbronn) method of tackling this type of problem. As an example, for $k_1 = k_2 = 2$, $k_3 = k_4 = 1$ Liu was only able to get an exponent of $(\sqrt{21} - 1)/5760 = 0.00062197.....$ Theorem 4 however, gives 1/16.

ibid. (3) 28 (1974) 385-401.

12. ———, "Sommes trigonometriques sur les nombres premiers", C.R. Acad. Sci. Paris Serie A 285 (1977) 981-983.

13. I.M. Vinogradov, "On the estimation of a trigonometric sum over primes", Izv. Akad. Nauk SSSR Ser. Mat. 12 (1948) 225-248.

14. G. L. Watson, "On indefinite quadratic forms in five variables", Proc. London Math. Soc. (3) 3 (1953) 170-181.

References for Chapter Five

1. A. Baker, "On some diophantine inequalities involving primes", J. Reine Angew. Math. 228 (1967) 166-81

1b. R.C. Baker & G. Harman, "Diophantine approximation by prime numbers", J. London Math. Soc.

2. H. Davenport & H. Heilbronn, "On indefinite quadratic forms in five variables", ibid. 21 (1946) 185-193.

3. H. Davenport & K.F. Roth, "The solubility of certain diophantine inequalities", Mathematika 2 (1955) 81-96.

4. G. Harman, "Trigonometric sums over primes I", Mathematika 28 (1981), 249-254.

5. ————, "Trigonometric sums over primes II", Glasgow Math. J. to appear.

The results used in Chapter five from the above two papers may be found in Chapter four.

6. M.C. Liu, "Recent development of some analogues of Waring's problem and Dirichlet's theorem involving primes", Southeast Asian Bull. Math. 3 (1979), 193-202.

7. H.L. Montgomery, "The analytic principle of the large sieve", Bull. Amer. Math. Soc. 84 (1978) 547-567.

8. K. Ramachandra, "On the sums $\Sigma \lambda_j f_j(p_j)$", J. Reine Angew. Math. 262/263 (1973), 158-165.

9. W. Schwarz, "Über die Lösbarkeit gewisser Ungleichungen durch Primzahlen", ibid. 212 (1963) 150-157.

10. R.C. Vaughan, "Diophantine approximation by prime numbers I", Proc. London Math. Soc. (3) 28 (1974) 373-384.

11. ————, "Diophantine approximation by prime numbers II",

SECTION TWO

SOME TOPICS IN MULTIPLICATIVE NUMBER THEORY

CHAPTER SIX INTRODUCTION TO SECTION TWO

In this second part of the thesis we shall be considering topics in multiplicative number theory. Each of chapters 7 - 10 consists of a preprint of one of my papers [5,6,7,8] . The present chapter contains some general results which are used repeatedly in the following chapters, but which are not quoted in an explicit form. There is also some general discussion on the background to the results and methods.

1. The background. Legendre was apparently the first mathematician to formulate a conjecture concerning $\pi(x)$. He proposed that

$$\pi(x) \simeq \frac{x}{\log x - 1.08...} . \qquad (1)$$

Gauss, however, while still a youth, concluded that $\pi(x)$ could be approximated by

$$\mathrm{li}\, x = \int_2^x \frac{dt}{\log t} .$$

The first general results to give weight to these conjectures were obtained by Tchebychev in 1851-2. He proved that

$$\liminf \frac{\pi(x)}{\mathrm{li}\, x} \leq 1 \leq \limsup \frac{\pi(x)}{\mathrm{li}\, x}$$

and

$$(0.92...)\frac{x}{\log x} < \pi(x) < (1.105...)\frac{x}{\log x}$$

for all sufficiently large x. Hadamard and de la Vallée Poussin independently, in 1896, proved the celebrated prime number theorem in the form

$$\pi(x) = \mathrm{li}\, x + O(x \exp(-c(\log x)^{\frac{1}{2}})) \qquad (2)$$

(see, for example, Chapter 18 of [3]). This shows that Legendre was wrong to conjecture (1), the 1.08... should be 1 . The important new feature of the work of Hadamard and de la Vallee Poussin was the demonstration that $\zeta(1 + it) \neq 0$ for any value of t . The only

improvement which has been made to (2) without any additional hypothesis is to increase the exponent $\frac{1}{2}$ on the logarithm (see [17]). On the Riemann Hypothesis, that all the complex zeros of $\zeta(s)$ lie on $\mathrm{Re}\, s = \frac{1}{2}$, the error term in (2) may be improved to $x^{\frac{1}{2}} (\log x)$. This is near to the best possible result since Littlewood showed that

$$\pi(x) - \mathrm{li}\, x = \Omega_{\pm}(x^{\frac{1}{2}} (\log\log\log x)(\log x)^{-1}) .$$

One question which naturally arises in view of the above results is : how evenly are the prime numbers distributed in short intervals ? That is, what can be said about

$$P(x,y) = \pi(x + y) - \pi(x)$$

where $y = o(x)$? From (2) it only follows that one can make a non-trivial statement concerning $P(x,y)$ if $y = \Omega(x \exp(-c(\log x)^{\frac{1}{2}}))$. Hoheisel [11] was the first to show that there exists an α less than 1 (he gave $\alpha = 1 - (3300)^{-1} + \varepsilon$) such that

$$P(x,x^{\alpha}) \sim \frac{x^{\alpha}}{\log x} \qquad \text{as} \quad x \to \infty . \quad (3)$$

This has subsequently been improved by Ingham, Montgomery and Huxley [14,18,12] . If $N(\sigma,T)$ denotes the number of zeros $\rho = \beta + i\gamma$ of the Riemann zeta function in the rectangle $|\gamma| \leq T$, $\beta \geq \sigma$, and

$$N(\sigma,T) << T^{\theta(1 - \sigma)} (\log T)^{A} \qquad \text{for} \quad \tfrac{1}{2} \leq \sigma \leq 1,$$

then the method of Ingham followed by subsequent authors shows that (3) holds for $\alpha > 1 - \theta^{-1}$. Huxley proved that $\theta \leq 12/5$ and so obtained $\alpha \geq 7/12 + \varepsilon$. The limit of these methods, even assuming the strongest possible hypotheses is $\alpha = \frac{1}{2}$. If one only requires (3) to be true for almost all x (in the sense that the measure of those $x \leq X$ for which (3) is untrue is $o(X)$) then Selberg [19] has shown that one may take $\alpha > 1 - 2\theta^{-1}$. In particular, Huxley's zero

form $N = p + P_2$, the method giving a similar approximation to question 2 above; Heath-Brown and Iwaniec [10] have shown that

$$P(x, x^{\alpha}) \quad >> \quad \frac{x^{\alpha}}{\log x}$$

for $\alpha > 11/20$. It is a common feature of sieve methods that one does not arrive at an asymptotic equality, but an upper or lower bound which is a multiple or fraction of the "expected" number.

One result of recent years which has been important in proving several results (like [10], [15]), is the improvement of the error term in the linear sieve (see Chapter 8 of [4] for the "old" form of the error term). This result is given by Iwaniec in [16], building on earlier work by Motohashi, Hooley and Chen. This work provides the starting point for chapters 8 and 9 of the present thesis. We write $|A_d|$ for the number of elements of A divisible by some squarefree integer d and we suppose that

$$|A_d| = \frac{\omega(d)\, X}{d} + r(A,d)$$

where X is a positive number independent of d, $\omega(d)$ is multiplicative with $0 \leq \omega(p) \leq p$ for $p \in P$, and $r(A,d)$ is considered to be an error term, small on average. Before the new form of the error term was available, the error term in the sieve ($R^{\pm}$ of Lemma 1 of chapter 8) was of the form

$$\sum_{\substack{d<D \\ d \mid P(z)}} |r(A,d)| \qquad (4)$$

where

$$P(z) = \prod_{\substack{p<z \\ p \in P}} p \ .$$

Sometimes each term in (4) was weighted with a factor $<< d^{\varepsilon}$. Since each term in (4) occurs in absolute value, there can be no cancellation of errors. Thus (4) limits the permissible size of the parameter D

density estimates gives $\alpha = 1/6 + \varepsilon$. The "classical" techniques used by the above authors are adapted to give the result of Chapter Seven here.

Of course, many other questions are raised concerning the distribution of prime numbers. The two well-known classical problems are

1. (Goldbach) Is every (or "every sufficiently large") even number the sum of two primes ?

2. Are there infinitely many prime twins ?

Another conjecture is

3. (Hardy-Littlewood) If a polynomial might reasonably be expected to represent a prime infinitely often (i.e. it is irreducible with no common divisor to its coefficients), does it in fact do so ?

Questions might also be asked about the distribution of primes in residue classes modulo q (see Chapter 15 of [18] for example). Recent progress in these problems have used sieve methods which we discuss briefly in the next section.

2. Sieve methods in prime number theory. The idea in an arithmetical sieve method (see [4] for a full account) is to remove (sift out) from a sequence of integers A, all numbers divisible by members less than z from a sequence of primes P. The members of A which remain will then only have prime divisors from P which are no less than z. In particular, depending on the relative sizes of z and the members of A, the elements of A which remain will not be divisible by "many" primes from P. In recent years sieve methods have been used with great success on problems mentioned in section 1, or on approximations to those problems. For example, Iwaniec [15] has shown that $n^2 + 1$ is a P_2 infinitely often; Chen [1] has shown that every sufficiently large even number N can be represented in the

although it is desirable to have D as large as possible (this is discussed more explicitly in chapters 8 and 9). Iwaniec replaced the sum in (4) with a multiple sum (see Lemma 1, Chapter 8) which allows for some cancellation of errors. The error term may be estimated by Fourier series and using standard methods for bounding exponential sums, or by using the Perron integral formula (see Lemma 1 below) and estimating mean values of Dirichlet polynomials. It is the latter procedure which will be used in chapters 8-10. Linnik's dispersion method can also be used (see [15]). By these methods cancellation is allowed for and so the value of D may be increased beyond the apparent natural limit imposed by (4).

Even though the value of the parameter D may now be taken nearly as large as the members of A in certain circumstances (compare the working in Chapter 9), it is apparently not possible by a sieve method alone to give a non-trivial lower bound for the number of primes in A. To do so would require D to be taken larger than the members of A. All the sieve method gives is either a non-trivial lower bound for the number of almost primes in A, or a lower bound (which is negative) for the number of primes less a certain subset of almost primes in A. The latter result is used in chapters 8 and 9 here. The important feature of this method is that classical analytic methods may be used successfully to give a lower bound for the number of almost-primes we have subtracted. The method presented in chapter ten is rather different, however, and here the sieve is employed to give an asymptotically "correct" result, while the Buchstab identity is used to decompose the original sifting function in such a manner that the only "awkward" sums that arise are non-negative and may be discarded.

3. Some fundamental results.

LEMMA 1 (The Perron Integral formula) Let

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad (\sigma > 1)$$

where $a_n = O(\psi(n))$, $\psi(n)$ being non-decreasing, and

$$(\sigma - 1)^{\alpha} \sum_{n=1}^{\infty} |a_n| n^{-\sigma} = O(1) \qquad \text{as} \quad \sigma \to 1.$$

Then, if $c > 0$, $c + \sigma > 1$, x is a positive number > 1, and N is the integer nearest to x, we have

$$\sum_{n<x} a_n n^{-s} = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} f(s+w) \frac{x^w}{w} \, dw +$$

$$+ O\left(x^c T^{-1} (c + \sigma - 1)^{\alpha} + \psi(2x) x^{1-\sigma} (\log x) T^{-1} + M\right)$$

where

$$M = \min\left(\psi(x) x^{-\sigma}, \psi(N) x^{1-\sigma} T^{-1} |x - N|^{-1}\right)$$

it being understood that $\psi(x) x^{-\sigma}$ is taken in the minimum if $x = N$.

Proof This is Lemma 3.12 of [20] essentially. In Chapters 7-10 it will be refered to as Lemma 3.12 of Titchmarsh's book.

LEMMA 2 (The fourth power moment of $\zeta(s)$) We have, for $T \geq 2$,

$$\int_1^T |\zeta(\tfrac{1}{2} + it)|^4 \, dt = (\tfrac{1}{2}) T \log^4 T \, \pi^{-2} + O(T \log^3 T).$$

Proof This result was first shown by Ingham [13]. In fact, much more is known (see [9]).

LEMMA 3 (The mean value theorem for Dirichlet polynomials) For any

real T_o and T we have

$$\int_{T_o}^{T_o+T} \Big| \sum_{n=1}^{N} a_n n^{-it} \Big|^2 dt = (T + \theta 4\pi N/3^{\frac{1}{2}}) \sum_{n=1}^{N} |a_n|^2$$

where $-1 \leq \theta \leq 1$.

Proof. This is theorem 6.1 of [18].

LEMMA 4 (Van der Corput's bounds for trigonometric sums) Let $f(x)$ be real and have continuous derivatives up to the kth order, where $k \geq 2$. Let $\lambda_k \leq f^{(k)}(x) \leq h\lambda_k$ (or $\lambda_k \leq -f^{(k)}(x) \leq h\lambda_k$). Let $b - a \geq 1$, $R = 2^{k-1}$. Then

$$\sum_{a \leq n \leq b} e(f(n)) \ll h^{2/R} (b-a) \lambda_k^{1/(2R-2)} + (b-a)^{1-2/R} \lambda_k^{-1/(2R-2)}.$$

Proof This is a combination of Theorems 5.9, 5.11 and 5.13 of [20].

4. Some additional results required for Chapter 9. In the preprint that forms Chapter 9 the main theorem involves a parameter h, and a proof is given only for the case $h = 0$. For $h \neq 0$ the proof follows a similar pattern, but we need to express the function $X(s)$ which occurs in terms of the Hurwitz zeta function. It is easily seen that the only properties of the Riemann zeta function used in Chapter 9 in connexion with $X(s)$ are : 1) Its appearance in the Perron integral formula; 2) The second and fourth power moments. The n^s occuring in Lemma 1 may be replaced by $(n+h)^s$ with the only alteration necessary being the term involving the nearest integer to x, where $|x - N - h|$ replaces $|x - N|$. The second and fourth power momemts of the Hurwitz zeta function may be estimated using its approximate functional equation (see [2]) and modifying the proof of the mean value theorem for Dirichlet polynomials. It should be noted that the behaviour of the Hurwitz zeta function deviates in many important aspects from that of the Riemann zeta function, but these do not enter

into the working as it affects $X(s)$.

5. The future ? None of the results in Chapters 7 - 10 are in what is believed to be their final form. The theorem of Chapter 7 is quite near to the "expected" result, however. There is some discussion in the other chapters on what details might be improved to get slightly better results. One frustrating respect of multiplicative number theory is that even on the strongest hypotheses, present methods are limited in many problems to giving results far worse than those believed to be best possible. For example, Cramér conjectured (as noted in Chapters 7 and 8) that every interval of the form

$$[n,\ n + f(n)\ (\log n)^2\ )$$

contains a prime, for some $f(n) \to 1$ as $n \to \infty$. Even on the Riemann hypothesis the interval length may not be reduced below $f(n)\ (\log n)\ n^{\frac{1}{2}}$. Similarly, in Chapter 9, the exponent $-\frac{1}{4}$ is the limit, even on the Riemann Hypothesis. It would be very desirable to have a new method, or a new plausible conjecture, that would push back these limits. To be plausible, of course, it must not lead to any results which contradict Littlewood's Ω result mentioned in section 1.

References to Chapter Six.

1. Chen, Jing-run, "On the representation of a large even integer as the sum of a prime and the product of at most two primes", Sci. Sinica 16 (1973), 157-176.

2. Cudakov, N., "On Goldbach-Vinogradov's theorem", Ann. Math., 48 (1947), 515-545.

3. Davenport, H., "Multiplicative Number Theory, second edition, Springer-Verlag, New York 1980 .

4. Halberstam, H. & Richert , H.-E., Sieve Methods, Academic Press London, 1974.

5. Harman, G., "Almost-primes in short intervals", Math. Ann. 258, 107-112 (1981).

6. ————, "Primes in short intervals", Math. Zeit., to appear.

7. ————, "The distribution of $\sqrt{p}$ modulo one", to appear.

8. ————, "On the distribution of αp modulo one ", J. London Math. Soc., to appear.

9. Heath-Brown, D.R., "The fourth power moment of the Riemann zeta function", Proc. London Math. Soc. (3) 38 (1979) 385-422.

10. ———— & Iwaniec, I., "On the difference between consecutive primes", Invent. Math. 55 (1979) 49-69.

11. Hoheisel, G. "Primzahlprobleme in der Analysis", Sitz Preuss. Akad. Wiss., 33 (1930), 3-11.

12. Huxley, M.N., "On the difference between consecutive primes", Invent. Math., 15, 164-170 (1972).

13. Ingham, A.E., "Mean value theorems in the theory of the Riemann

zeta-function", Proc. London Math. Soc. (2) 27 (1926) 273-300.

14. ————, "On the difference between consecutive primes", Quart. J. Math. Oxford, 8 (1937), 255-266.

15. Iwaniec, H., "Almost-primes represented by quadratic polynomials" Invent. Math. 47 (1978), 171-188.

16. ————, "A new form of the error term in the linear sieve" Acta Arithmetica 37 (1980) 307 320.

17. Korobov , "Estimates for trigonometric sums and their applications" (Russian), Uspehi Mat. Nauk 13 (1958), 82, 185-192.

18. Montgomery, H.L., Topics in multiplicative number theory, Berlin Springer 1971.

19. Selberg, A. "On the normal density of primes in short intervals and the difference between consecutive primes", Arch. Math. Naturvid. 47 (1943) 87-105.

20. Titchmarsh, E.C., Theory of the Riemann zeta-function. Oxford 1951.

CHAPTER SEVEN

ALMOST - PRIMES IN SHORT INTERVALS

1. Introduction.

Assuming the Riemann Hypothesis, Selberg [8] has shown that, for almost all n, the interval $[n, n + f(n) \log^2 n]$ contains a prime, providing $f(n) \to \infty$ with n. Here "almost all n" indicates that the number of exceptional n is $o(n)$. It is convenient to extend this definition to a real variable y so that "almost all y" signifies that the measure of the exceptional set is $o(y)$. Cramér conjectured [1] that every interval of the above form contains a prime where $f(n) \to 1$ as $n \to \infty$. The best unconditional results to date are due to the present author [2] and Heath-Brown and Iwaniec [5] who show that almost all intervals of the form $[n, n + n^{\frac{1}{10}}]$ and every interval of the form $[n, n + n^{11/20 + \varepsilon}]$ contain a prime, respectively. If we only ask for an interval to contain a P_2, i.e. a number with two prime factors, a much stronger unconditional result is possible. Using a sieve method Heath-Brown [3] proved that almost all intervals of the form $[n, n + n^{1/11}]$ contain a P_2. Y. Motohashi [7], by a simple analytic method reduced the required interval length to n^{ε}, and Wolke [11] improved this to $(\log n)^C$ where C is a sufficiently large constant (he quotes 5.10^6). It seems interesting that the value of C may be reduced to single figures by modifying Wolke's method. Here we prove:

THEOREM *Let $\delta > 0$ be given. Then almost all intervals of the form*

$$[\, n,\ n + (\log n)^{7+\delta} \,] \tag{1}$$

contain a P_2 number.

I should like to express my gratitude to R.C. Baker for suggesting this problem to me and furnishing me with a simple proof of Lemma 3 below. I would also thank the referee for his helpful suggestions, which have made the paper easier to read.

2. Notation and preliminary lemmas.

Constants implied by the o, O and $\ll$ conventions will depend at most on δ. We suppose x to be a sufficiently large positive number and y to satisfy $x \leq y \leq 2x$. We write $\rho = \beta + i\gamma$ for a zero of the Riemann zeta-function and

$$N(\sigma, T) = \sum_{\substack{\rho \\ \beta \geq \sigma, |\gamma| \leq T}} 1$$

We put

$$L = \log x , \qquad L_2 = \log\log x , \qquad T = xL^{10} ,$$

$$U = [3xL^{-7-\delta}] + 1/4 , \qquad P(s) = \sum_{U<n<2U} \Lambda(n) n^{-s} ,$$

$$\Phi(y) = \sum_{\substack{y<nn' \leq y(1+U^{-1}) \\ U<n<2U}} \Lambda(n)\,\Lambda(n') , \qquad \theta(s) = \frac{1}{s}\left(\left(1 + \frac{1}{U}\right)^s - 1\right) ,$$

$$M(s) = \min(1, U|s|^{-1}) , \qquad \lambda = 3/14 - \delta/100 ,$$

$$J(s) = M(s)^2 |P(s)x^s|^2 , \qquad H(y,n) = \|y/n\|^{-1} + \|y(1+U^{-1})/n\|^{-1} .$$

Here $\| \ \|$ denotes distance to the nearest integer. For $s = \sigma + it$, $-1 < \sigma < 2$ we note that

$$\theta(s) \ll M(s)\, U^{-1}$$

and we also observe that $P(1) = \ell n 2 + o(1)$.

LEMMA 1 We have

$$N(\sigma, V) \ll V^{\tau(1-\sigma)} (\log V)^{10} \text{ when } \sigma \geq 1-\lambda \tag{2}$$

where $\tau = \tau(\delta) < 2$;

$$N(\sigma, V) = 0 \text{ for } \sigma \geq 1 - (\log V)^{-3/4} \tag{3}$$

providing $V \geq L$ and x is sufficiently large;

$$N(\sigma, V+1) - N(\sigma, V) \ll \log V \text{ for } V \geq 2. \tag{4}$$

Proof The result (2) may be deduced from Theorem 1 of [4] when $\sigma \leq 49/50$. For $\sigma > 49/50$ we may use Theorem 12.3 of [6] together with Theorem 5.14 of [9] (with $\ell = 6$). A stronger result than (3) is given on page 226 of [10]. Theorem 9.2 of [9] gives the well known result (4).

LEMMA 2 For almost all y

$$\sum_{U<n<2U} \frac{\Lambda(n)}{n} \min(H(y,n), n^2) \ll \frac{x L^2}{U} \tag{5}$$

Proof We note that, for $U < n < 2U$,

$$\frac{1}{x}\int_x^{2x} \min(\|y/n\|^{-1}, n^2)\, dy \ll \int_0^n \min(\tfrac{1}{t}, n)\, dt \ll L .$$

The result (5) clearly follows for almost all y.

LEMMA 3 Let points λ_j $(j = 1,\ldots,N)$ be given in $[0,1)$. Then there is a set $S \subset [0,1)$ of measure $\geq 1/2$ such that

$$\max_{t \in S} \sum_{j=1}^{N} |t - \lambda_j|^{-1} \ll N \log N .$$

Proof Let Q be the subset of $[0,1)$ for which $|t - \lambda_j|^{-1} \leq N^2$ $(j = 1,..N)$. Then Q has measure $\geq 1 - 2N^{-1}$ and

$$\int_Q \sum_{j=1}^{N} |t-\lambda_j|^{-1}\, dt < 2N \int_{N^{-2}}^{1} \frac{dt}{t} = 4N \log N .$$

The result of this lemma easily follows .

LEMMA 4 Suppose $|\rho| \ll T$. Then

$$P(\rho) = P_1(\rho) + P_2(\rho)$$

where

$$P_1(\rho) \ll U^{1-\beta}(1+|\gamma|)^{-1} + U^{-\beta} L^2$$

and

$$P_2(\rho) \ll \sum_{\substack{\rho' \\ |\gamma-\gamma'|\leq U}} \frac{U^{\beta'-\beta}}{1+|\gamma'-\gamma|} .$$

Proof This follows from Lemma 2 of [11], modified by changing $U^{\varepsilon/2}$ there to U.

LEMMA 5 We have

$$\sum_{\substack{x\leq nn'\leq 2x \\ U<n<2U \\ n,n' \text{ not both primes}}} \Lambda(n)\Lambda(n') \ll x L^{-7/2} .$$

Proof The sum on the left above is

$$\ll \sum_{2\leq k<2L} U^{1/k-1} x + \sum_{2\leq k<15L_2} (x/U)^{1/\ell-1} x$$

$$\ll x L^{-7/2} \quad \text{as required.}$$

3. Proof of Theorem

We write E for the interval $[1-\lambda,\ 1-\lambda+L_2^{-1}]$. For any value of t with $|t| \leq T$ we let ℓ_σ denote the vertical line joining $\sigma+ti$

and $\sigma + (t+1)i$. For each zero ρ with $t-1 \le \gamma \le t+1$ we write $\lambda_\rho = (\beta - (1-\lambda))L_2$ if $\beta \in E$, $\lambda_\rho = 0$ if $\beta \le 1-\lambda$, $\lambda_\rho = 1$ if $\beta \ge 1 - \lambda + L_2^{-1}$. By (4) there are $\ll L$ such points λ_ρ. We conclude, using Lemma 3, that there is a subset E_o of E, of measure $\ge L_2^{-1}/2$, such that

$$\sum_{|s-\rho|\le 1} |s-\rho|^{-1} \le L_2 \sum_{|s-\rho|\le 1} |\lambda_\rho - (\sigma - (1-\lambda))L_2|^{-1} \ll L L_2^2 \qquad (6)$$

for $s \in \ell_\sigma$, $\sigma \in E_o$.

Since E_o has measure $\ge L_2^{-1}/2$, there exists $\sigma \in E_o$ such that

$$\int_{\ell_\sigma} J(s)\,|ds| \le 2L_2 \int_{E_o}\int_{\ell_\sigma} J(s)\,|ds|d\sigma \ll L_2 \int_E \int_{\ell_\sigma} J(s)|ds|d\sigma$$

Similarly, for a given value t, we may pick w with $t - \frac14 \le w \le t + \frac14$ and, if ℓ_w is the horizontal line from $1-\lambda+iw$ to $1-\lambda+L_2^{-1}+iw$,

$$\int_{\ell_w} J(s)\,|ds| \ll \int_E \int_{(w-\frac18)i+\sigma}^{(w+\frac18)i+\sigma} J(s)\,|ds|d\sigma,$$

and (6) holds for $s \in \ell_w$. We can thus make up a contour C, from parts of such lines from $\sigma_1 - iT$ to $\sigma_2 + iT$ where $\sigma_j \in E$ $(j = 1,2)$ so that

$$\int_C J(s)\,|ds| \ll L_2 \int_E \int_{-T}^{T} J(\sigma + it)\,dt\,d\sigma .$$

Also, by (6) and Theorem 9.6 (A) of [9],

$$\frac{\zeta'}{\zeta}(s) \ll L L_2^2 \quad \text{for } s \in C.$$

Henceforth we assume $\|y/n\| > 0$, $\|y(1+U^{-1})/n\| > 0$, for $U < n < 2U$. Put $c = 1 + L^{-1}$. Then, by Lemma 3.12 of [9] we have

$$\Phi(y) = \sum_{U<n<2U} \frac{\Lambda(n)}{2\pi i} \int_{c-iT}^{c+iT} -\frac{\zeta'}{\zeta}(s)\,\frac{\theta(s)\,y^s}{n^s}\,ds \qquad (7)$$

$$+ O\Big(\sum_{U<n\le 2U} \Lambda(n)\,(xL^2/(Tn) + \min(xLH(y,n)/(nT), n))\Big).$$

Hence, by changing the path of integration in (7) and using Lemma 2, for almost all y we have

$$\Phi(y) = \frac{y}{U} P(1) - \sum_{\rho}' P(\rho)\theta(\rho)\, y^{\rho} - \frac{1}{2\pi i}\int_{C} \frac{\zeta'}{\zeta}(s)\theta(s) P(s)\, y^{s}\, ds$$

$$+ O(xU^{-1}L^{-1})$$

$$= yU^{-1} P(1) - S_y - I_y/2\pi + O(xU^{-1}L^{-1}) \quad \text{say.} \tag{8}$$

In the above we have written Σ' to indicate summation over zeros with $|\gamma| \leq T$ to the right of the contour C.

We now consider

$$I = \frac{1}{x^2}\int_{x/2}^{3x/2}\int_{h}^{2h} |I_y|^2\, dy\, dh .$$

Clearly if

$$I \ll (x/U)^2 L_2^{-4} \tag{9}$$

then $I_y \ll L_2^{-1}(x/U)$ for almost all y.

By integrating first with respect to y then h we find that

$$I \ll \frac{L_2^4 L^2}{U^2}\int_{C} |ds|\, |P(s) M(s) x^{s}| \int_{C} \frac{|dw|\, |P(w)M(w)x^{w}|}{(1 + |Im(s) - Im(w)|)^2}$$

$$\ll \frac{L_2^4 L^2}{U^2}\int_{C} J(s)|ds|$$

$$\ll \frac{L_2^5 L^2}{U^2}\sum_{r=-\infty}^{\infty} \frac{1}{1+r^2}\int_{E}\int_{rU}^{(r+1)U} x^{2\sigma} |P(\sigma + it)|^2\, dt\, d\sigma$$

$$\ll \frac{x^2 L_2^5 L^3}{U^2}\left(\frac{x}{U}\right)^{-2\lambda} \qquad \text{by Theorem 6.1 of [6] .}$$

$$\ll L^6 \left(\frac{x}{U}\right)^2 \max_{\beta_1,\beta_2,\beta_3} U^{\beta_2+\beta_3-2\beta_1} x^{2\beta_1-2} N(\beta, 2T) \qquad (12)$$

where $\beta = \max(\beta_1,\beta_2,\beta_3)$. Here we have split the triple sum over zeros into three sums corresponding to $\beta = \beta_1, \beta_2$ or β_3 and summed over ρ_1, ρ_2 or ρ_3 last, respectively. The expression in (12) is an increasing function of β_j if $\beta_j < \beta$. Thus the expression in (12) is

$$\ll L^6 \left(\frac{x}{U}\right)^2 \max_{\beta} x^{2\beta-2} N(\beta, 2T)$$

$$\ll \left(\frac{x}{U}\right)^2 L^{-1} \qquad (13)$$

using (2), and (3). Combining (10), (11), (13) gives

$$S_y \ll (x/U) L_2^{-1}$$

for almost all y as required to finish the proof.

This establishes (9) since $2\lambda(7+\delta) > 3$. It remains to prove that S_y is $O(xU^{-1}L_2^{-1})$ for almost all y, because (8) then implies that $\Phi(y) \geq y\,P(1)/2U$ for almost all y. It follows that $\Phi(n) \geq n\,P(1)/2U - LL_2$ for almost all $n \in [x, 2x]$. By Lemma 5 the contribution to $\Phi(n)$ from integers which are not P_2s is of a smaller order for almost all n, which completes the proof.

We write

$$S_y = S_y^{(1)} + S_y^{(2)} + S_y^{(3)} .$$

Here

$$S_y^{(1)} = \sum_{|\gamma| \leq L^8} y^{\rho} P_1(\rho)\,\theta(\rho) \ll \sum_{|\gamma| \leq L^8} \frac{x^{\beta-1} U^{1-\beta}}{1+|\gamma|} \left(\frac{x}{U}\right)$$

$$\ll (x/U)L_2^{-1} \tag{10}$$

using (2) and (3). We have written $S_y^{(2)}$ for the sum involving $P_1(\rho)$ with $|\gamma| > L^8$ and $S_y^{(3)}$ for the sum involving $P_2(\rho)$. We have

$$\frac{1}{x}\int_x^{2x} |S_y^{(2)}|^2\,dy \ll L^2 \sum_{|\gamma| > L^8} |P_1(\rho)|^2 \left(\frac{x}{U}\right)^2 x^{2\beta-2}$$

$$\ll \left(\frac{x}{U}\right)^2 L^{-3} \tag{11}$$

from (2) and (3) .

Also

$$\frac{1}{x}\int_x^{2x} |S_y^{(3)}|^2\,dy \ll L^2 \sum_{|\gamma| \leq T} |P_2(\rho)|^2 \left(\frac{x}{U}\right)^2 x^{2\beta-2}$$

$$\ll L^2 \sum_{\substack{\rho_j \\ |\gamma_j| \leq T}} \sum \sum \frac{U^{\beta_2+\beta_3-2\beta_1} x^{2\beta_1-2}}{(1+|\gamma_1-\gamma_2|)(1+|\gamma_1-\gamma_3|)} \left(\frac{x}{U}\right)^2$$

CHAPTER EIGHT

PRIMES IN SHORT INTERVALS

1. Introduction

It was conjectured by Cramér [1] that every interval of the form $[n, n + f(n) \log^2 n]$ contains a prime for some $f(n) \to 1$ as $n \to \infty$. Assuming the Riemann Hypothesis, Selberg [12] has shown that almost all intervals of the above form contain a prime providing $f(n) \to \infty$ with n. "Almost all" in this context indicates that the number of $n \leq X$ for which the statement is false is $o(X)$. Selberg's proof essentially gave a relationship between the density of zeros of $\zeta(s)$ and the length of the interval. This was used by Montgomery (Chapter 14 of [11]) to show that, for almost all n, $[n, n^{1/5 + \varepsilon}]$ contains a prime. The exponent $1/5$ may be improved to $1/6$ using the zero density estimate of Huxley [6] which he obtained to show that $p_{n+1} - p_n \ll p_n^{7/12 + \varepsilon}$ where p_n is the nth prime. This result on the difference between consecutive primes has been improved by Iwaniec and Jutila [8] to $p_n^{5/9 + \varepsilon}$, and by Heath-Brown and Iwaniec [5] to $p_n^{11/20 + \varepsilon}$. These last two results were obtained by a sieve method. We shall use similar arguments to prove the following result:

THEOREM *For almost all* n, *the interval*

$$[n, n + n^{(1/10) + \varepsilon}) \tag{1}$$

contains a prime number.

It is the hypothesis of Lemma 5 below which sets $(1/10) + \varepsilon$ as the limit of the present method. We shall in fact

References

1. Cramér, H. : On the order of magnitude of the difference between consecutive prime numbers. Acta Arith. 2 (1937), 23-46.

2. Harman, G. : Primes in short intervals, to appear.

3. Heath-Brown, D.R. : Almost-primes in arithmetic progresions and short intervals. Math. Proc. Camb. Phil. Soc. 83 (1978) 357-375.

4. : Zero density estimates for the Riemann Zeta-function and Dirichlet L-functions. J. London Math. Soc. (2) 19 (1979) 221-232.

5. and H. Iwaniec : On the difference between consecutive primes. Invert. Math. 55 (1979) 49-69.

6. Montgomery, H.L. : Topics in multiplicative number theory. Berlin: Springer 1971.

7. Motohashi, Y. : A note on almost-primes in short intervals. Proc. Japan Acad. Ser. A Math. Sci. 55 (1979), 225-226.

8. Selberg, A. : On the normal density of primes in short intervals, and the difference between consecutive primes. Arch. Math. Naturvid. 47 (1943) 87-105.

9. Titchmarch, E.C. : Theory of the Riemann Zeta-function. Oxford 1951.

10. Walfisz, A. : Weylsche Exponential summen in der neuren Zahlentheorie. Berlin : Deutscher Verlag der Wiss, Berlin, 1963.

11. Wolke, D. : Fast-Primzahlen in kurzen intervallen, Math. Ann. 244, 233-242 (1979).

Royal Holloway College,
EGHAM,
Surrey. TW20 OEX
England.

show that for almost all n the interval (1) contains $\gg n^{(1/10)+\epsilon}(\log n)^{-1}$ primes. This exhibits a common feature of sieve results: we obtain a lower bound which is a fraction of the "expected" number of primes under consideration.

2. Outline of Method

In sections 2-4 we use the following standard notation:

$$P(z) = \prod_{p<z} p \quad , \qquad V(z) = \prod_{p<z} (1 - 1/p) \ ,$$

and note the well known asymptotic formula:

$$V(z) = \frac{e^{-\gamma}}{\log z} + O((\log z)^{-2}) \tag{2}$$

where γ is Euler's constant. For a finite set of integers A write

$$A_d = \{n \in A ; \ d|n\}$$

$$S(A,z) = |\{n \in A, \ (n, P(z)) = 1\}| .$$

We shall consider the set

$$A = \{ n; \ x - y < n \leq x \} .$$

Here x is a real number satisfying $X < x \leq 2X$, where X will be assumed "large", and $y = xX^{-(9/10)+\varepsilon/2}$. The fundamental Buchstab identity states that

$$S(A,z_1) = S(A,z_2) - \sum_{z_1 \leq p < z_2} S(A_p,p) \ .$$

Using this we find that, for $z_1 < z_2 < x^{\frac{1}{2}}$, we have

$$\pi(x) - \pi(x-y) = S(A, x^{\frac{1}{2}})$$

$$= S(A, z_1) - \sum_{z_1 \leqslant p < x^{\frac{1}{2}}} S(A_p, p)$$

$$= S(A, z_1) - \sum_{z_2 \leqslant p < x^{\frac{1}{2}}} S(A_p, z_3(p)) - \sum_{z_1 \leqslant p < z_2} S(A_p, z_4(p))$$

$$+ \sum_{\substack{z_3(p) \leqslant q < p < x^{\frac{1}{2}} \\ p \geqslant z_2}} S(A_{pq}, q) + \sum_{\substack{z_4(p) \leqslant q < p < z_2 \\ p > z_1}} S(A_{pq}, q)$$

$$= \Sigma_1 - \Sigma_2 - \Sigma_3 + \Sigma_4 + \Sigma_5 \quad \text{say.}$$

In the above it is also necessary to have $z_3(p) \leqslant p$ for $p > z_2$, $z_4(p) \leqslant p$ for $z_1 \leqslant p < z_2$. Since we will only give a lower bound for $\pi(x) - \pi(x-y)$ we shall consider Σ_2 with $x^{\frac{1}{2}}$ replaced with $(2X)^{\frac{1}{2}}$, and Σ_4 with $x^{\frac{1}{2}}$ replaced by $X^{\frac{1}{2}}$. Then

$$\pi(x) - \pi(x-y) \geqq \Sigma_1 - \Sigma_2 - \Sigma_3 + \Sigma_4 + \Sigma_5. \qquad (3)$$

We shall give a lower bound for Σ_1 and an upper bound for Σ_2 and Σ_3 by means of the linear sieve (Lemma 1). It should be noted that one can make use of certain subsums over almost-primes which arise in the sieve results in [7] to improve the lower bound for the left hand side of (3). The inclusion of these sums has significance in other problems, but is unnecessary here. We deal with the remainder terms in Lemma 1 by bounding the integral of their square over $[X, 2X]$, using Dirichlet polynomials (see Lemmas 2 - 6). The motivating principle here is to be able to choose the D which occurs in Lemma 1 as large as possible. To this end we shall pick z_1, z_2, $z_3(p)$, $z_4(p)$ so that the hypotheses for our estimates of mean values of Dirichlet polynomials match the form of the remainder term given by

Iwaniec. Eventually we obtain a lower bound of the form $C'y/\log X$ for $\Sigma_1 - \Sigma_2 - \Sigma_3$, valid for all x except on a set of measure $o(X)$. Here C' is negative, but quite small. On the other hand, we are able to give an asymptotic formula for a subsum of Σ_4, with an error which is also considered by its integral over $[X, 2X]$.

The remainder of the sum, together with the whole of Σ_5, being non-negative, is discarded.

This leads to a lower bound of $C'' y/\log X$, where $C'' + C' > 0$.

In proving the theorem we may, of course, assume that the ε in (1) is "sufficiently small". We use ϕ for a positive function of ε, and henceforth reserve the letter C for an absolute constant. We write λ for $(\log X)^B$ where B is bounded by a function of ε. The entities ϕ, C, λ need not be the same at each occurrence. We may thus write, for example,

$$(X^{\phi})^{\varepsilon} \gg X^{\phi}, \quad \text{or} \quad \lambda^3 \ll \lambda .$$

The constants implied by Vinogradov's $\ll$ notation depend here, and elsewhere in this paper, on at most ε. We write

$$T = X^{9(1-\varepsilon)/10}, \quad Y = X^{(1/10)+\varepsilon}, \quad z_1 = X^{26(1-3\varepsilon)/105},$$

$$z_2 = X^{9/35}, \quad z_3(p) = (X^{1-3\varepsilon}/p)^{1/3}, \quad z_4(p) = (X^{(26/35)-2\varepsilon}/p)^{\frac{1}{2}}.$$

The reason for this particular choice of z_1, z_2, z_3, z_4 will become apparent in section 5 when the remainder term of the sieve is estimated.

LEMMA 1. Let $z \geq 2$, $D \geq z^2$ and $\varepsilon > 0$. Then

$$S(A,z) \leq WV(z)\{F(s) + E\} + R^+ \tag{5}$$

$$S(A,z) \geq WV(z)\{f(s) - E\} - R^- \tag{6}$$

where $s = (\log D/(\log z)$ and $E = C\epsilon + O((\log D)^{-1/3})$. The remainder terms $R^{\pm}$ are of the form

$$R^{\pm} = \sum_{(D)} R^{\pm}_{(D)} = \sum_{(D)} \sum_{\nu<D^{\varepsilon}} C^{\pm}_{(D)}(\nu,\varepsilon) \sum'_{D_i \leq p_i \leq D_i^{1+\varepsilon^7}} r(A,\nu p_1 \ldots p_r) \tag{7}$$

where (D) runs over all subsequences $D_1 \geq D_2 \ldots \geq D_r$, including the empty subsequence, of the sequence

$$D^{\varepsilon^2(1+\varepsilon^7)^n}, \qquad n \geq 0,$$

for which

$$D_1 D_2 \ldots D_{2k} D_{2k+1}^3 \leq D \qquad (0 \leq k \leq (r-1)/2)$$

in the case of R^+, and

$$D_1 D_2 \ldots D_{2k-1} D_{2k}^3 \leq D \qquad (0 \leq k \leq r/2)$$

in the case of R^-. Moreover, Σ' indicates that ν and p_i, $(1 \leq i \leq r)$, are restricted by the conditions

$$\nu \mid P(D^{\varepsilon^2}), \quad p_i \mid P(z).$$

Finally, the coefficients $C^{\pm}_{(D)}(\nu,\varepsilon)$ depend at most on (D), ν, ε and the $\pm$ signs and satisfy

$$|C^{\pm}_{(D)}(\nu,\varepsilon)| \leq 1.$$

3. The fundamental sieve result

We use the linear sieve result of Iwaniec [7] in the form stated in [5]. When we come to apply Lemma 1, the A occurring in its statement will not always be that specified in section 2. For the properties of the standard functions $f(s)$ and $F(s)$ see [2] (Chapter 8). We write

$$r(A,d) = |A_d| - W/d$$

for the remainder term, where W is independent of d.

4. Some preliminary results

In this section we give the relation between the remainder terms and integrals of Dirichlet polynomials, and various estimates for such integrals. For any upper case latin letter B other than Q, P, and H we write

$$B(s) = \sum_{B<b\leq 2B} \alpha_n b^{-s}$$

where α_n is real and $\sum_{B<b\leq 2B} \alpha_n^k \ll B^{\lambda}$, for any integer $k \leq C_1(\varepsilon)$.

For the letters L,K we stipulate other conditions. For both K and L $\alpha_n = 1$ for some set of consecutive integers and $\alpha_n = 0$ otherwise. For L the condition $L < \ell \leq 2L$ is to be replaced by $C_2(\varepsilon) \leq \ell/L \leq C_3(\varepsilon)$.

For $1 \ll H \ll D^{\epsilon}$ we define $H^{\pm}(s)$ by

$$H^{\pm}(s) = \sum_{H\leq \nu<2H} C^{\pm}_{(D)}(\nu,\varepsilon)\, \nu^{-s}$$

For numbers P_j $(j = 1,\ldots r)$ with $D_j \leq P_j \leq D_j^{1+\epsilon^7}$ we write

$$P_j(s) = \sum_{P_j\leq p_j<2P_j} P_j^{-s}\, \alpha^{(j)}_{p_j}$$

where $\alpha_n^{(j)} = 1$ for some set of consecutive integers n, and is zero otherwise.

We write $R^{\pm}_{(D)}(H, P_1,\ldots,P_r)$ for that subsum of $R^{\pm}_{(D)}$ corresponding to $P_j \leq p_j < 2P_j$. To consider $R^{+}_{(D)}$ for Σ_2 we put

$$P(s) = \sum_{\substack{P\leq n<2P \\ n<(2X)^{\frac{1}{2}}}} n^{-s}\, \Lambda(n)/(\log P)$$

for any number P with $z_2 \leqslant P < (2X)^{\frac{1}{2}}$. We replace A by A_n in (5) and write $R^{+}_{(D)}(P, H, P_1, \ldots, P_r)$ for the sum of the remainder terms $R^{+}_{(D)}(H, P_1, \ldots, P_r)$ weighted with the factor $\Lambda(n)/(\log P)$ for $P \leqslant n < \min(2P, (2X)^{\frac{1}{2}})$. We use the same notation for the remainder terms from Σ_3, replacing $(2X)^{\frac{1}{2}}$ by z_2 and z_2 by z_1.

Also we write

$$H(s) = \min\left(\frac{X^{9/5}}{|s|^2+1}, 1\right),$$

$$c = 1 + (\log X)^{-1}.$$

LEMMA 2 *For any continuous function* $g(s)$, *and* $0 < T_o < T < X$, *we have*

$$\frac{1}{X}\int_{X}^{2X}\left|\int_{c+iT_o}^{c+iT} g(s)\, x^s\, ds\right|^2 dx$$

$$\ll X^2(\log X)\int_{c+iT_o}^{c+iT} |g(s)|^2\, |ds|.$$

Proof This is easily established by squaring out the inner integral on the left, integrating with respect to x first and making use of the inequality:

$$|g(c+it_1)\, g(c+it_2)| \leq |g(c+it_1)|^2 + |g(c+it_2)|^2.$$

LEMMA 3 *Suppose* $YX^{-\varepsilon} \leq A \leq X^{1-\varepsilon}$, *then*

$$\sum_{A<n\leq 2A} a_n\left([\tfrac{x}{n}] - [\tfrac{x-y}{n}]\right) = y\sum_{A<n\leq 2A}\frac{a_n}{n} + O(yX^{-\phi}) + I$$

where

$$I = \frac{1}{2\pi i}\left(\int_{c-iT}^{c-iT_o} + \int_{c+iT_o}^{c+iT}\right) L(s)\, A(s)\, \frac{x^s - (x-y)^s}{s}\, ds.$$

Here $L = X/A$, $T_o = L^{\frac{1}{2}}$, $C_2(\varepsilon) = \frac{1}{3}$, $C_3(\varepsilon) = 3$.

Proof This is demonstrated in all essentials in [5], pp. 53-54.

COROLLARY (1) Write $L = X(H P_1 \ldots P_r)^{-1}$. Let A be as in section 2 and let $W = y$. Then we have, for $D = X^{1-3\epsilon}$

$$\frac{1}{X}\int_X^{2X} |R^{-}_{(D)}(H, P_1, \ldots P_r)|^2 \, dx$$

$$\ll Y^2 \lambda \int_{c+iT_o}^{c+iT} H(s) \, |H^{-}(s)L(s)P_1(s)\ldots P_r(s)|^2 |ds| + Y^2 X^{-\phi}. \qquad (8)$$

For $T_o = L^{\frac{1}{2}}$.

COROLLARY (2) Write $L = X(H P P_1 \ldots P_r)^{-1}$. Replace A by A_n, put $D = X^{1-3\epsilon}/P$, $z = z_3(2P)$ for Σ_2, $z = z_4(2P)$ for Σ_3, and let $W = y/n$. Then we have

$$\frac{1}{X}\int_X^{2X} |R^{+}_{(D)}(P, H, P_1, \ldots P_r)|^2 \, dx$$

$$\ll Y^2 \lambda \int_{c+iT_o}^{c+iT} H(s) |H^{+}(s)L(s)P(s)P_1(s)\ldots P_r(s)|^2 \, |ds| + Y^2 X^{-\phi}. \qquad (9)$$

The above corollaries follow by combining Lemmas 2 and 3 and using the definition of the remainder terms.

We write $T_1 = X^{9/10 - \epsilon}$ and note that the presence of the $H(s)$ factors in (8) and (9) indicate that it suffices to consider integrals from $c + iT_2$ to $c + iT_3$ where $T_3 - T_2 \leq T_1$ and $T_2 \geq T_o$. We write I for such a line of integration.

We note that the classical mean value theorem for Dirichlet Polynomials (Theorem 6.1 of [11]) gives, for a positive integer h,

$$\int_I |M(s)|^{2h} \, |ds| \ll \lambda (1 + T/M^h) \qquad (10)$$

This result shall be used repeatedly in the following. The next lemma gives a bound for integrals of the above type when h is not an integer, and lemma 5 continues in a similar vein.

$$\max_{s\in I} |K(s)| < X^{-\phi}, \tag{13}$$

This, together with (11) for $h = 3$ gives the following :

COROLLARY *If* $K > T_1^{2/7} X^{\varepsilon/10}$ *then*

$$\int_I |K(s)|^8 |ds| << X^{-\phi}.$$

LEMMA 5 *Suppose* $KMN \geq T_1^{10/9} X^{\varepsilon/10}$, $K \geq X^{\varepsilon}$, $N >> X^{\varepsilon^2/2}$, *and* $\max(KM, MN) \geq T_1^{6/7} X^{\varepsilon}$. *Then*

$$\int_I |K(s)\, M(s)\, N(s)|^2 |ds| << X^{-\phi}.$$

Proof We assume $KM \geq MN$, the other case follows similarly. We write $J(\alpha)$ for the largest even integer $\leq \alpha$, and define β to be the smallest number not less than 8 for which

$$N^{\beta+J(\beta)} \geq T_1^4. \tag{14}$$

We put $\tau = 2\beta\,(\beta-2)^{-1}$, then, by Hölder's inequality

$$\int_I |K(s)\, M(s) N(s)|^2 |ds| \leq \left(\int_I |N(s)|^{\beta} |ds|\right)^{2/\beta} \left(\int_I |K(s)\, M(s)|^{\tau}\right)^{2/\tau}. \tag{15}$$

From (14) and (11) with $h = J(\beta)/2$, together with $|N(s)| << \lambda$, it follows that

$$\int_I |N(s)|^{\beta} |ds| << \lambda. \tag{16}$$

We now apply lemma 4 to $K(s)\,M(s)$ with τ in place of β and $h = 1$. Using (13) and $|M(s)| << \lambda$ we obtain the inequality

$$\int_I |K(s)M(s)|^{\tau} |ds| << X^{-\phi}, \tag{17}$$

LEMMA 4 *Let* h *be an integer* ≥ 1 *and* β *a real number with* $6h > \beta > 2h$. *Then*

$$\int_I |M(s)|^\beta \, |ds| \ll \lambda\left(\mu + \left(\frac{T_1}{M^{2h}\mu}\right)^{(\beta-2h)/(6h-\beta)}\left(1 + \frac{T_1}{M^h}\right)\right) \tag{11}$$

where μ *is any number* $\geq \max_{s\in I} |M(s)|^{(\beta-2h)}$.

Proof Put $Q(s) = M(s)^h$, $Q = M^h$. Let s_r be any points in I with $|s_j - s_k| \geq 1$ for $j \neq k$, and $V < |Q(s_r)| \leq 2V$ $(r = 1,\ldots R)$. By the form of the Halász lemma due to Huxley [6] we have

$$R \ll \lambda(V^{-2} + T_1 Q^{-2} V^{-6}) .$$

Thus

$$R V^{2+(\beta-2h)/h} \ll \lambda(V^{(\beta-2h)/h} + T_1 Q^{-2} V^{-4 + (\beta-2h)/h})$$

$$\ll \lambda \mu$$

providing

$$V \geq \left(\frac{T_1}{M^{2h}\mu}\right)^{h/(6h-\beta)} . \tag{12}$$

If (12) holds it follows that the integral over that part of I for which $|Q(s)| > V$ is $\ll \lambda\mu$. For the remainder of the integral it follows from (10) that we get the bound

$$\ll \left(\frac{T_1}{M^{2h}\mu}\right)^{(\beta-2h)/(6h-\beta)}\left(1 + \frac{T_1}{M^h}\right).$$

Which completes the proof of (11). It should be noted that this result is considerably weaker than what might be expected (cf. Conjecture 9.2 of [11]).

By Van der Corput's bounds for exponential sums (see Chapter 5 of [13] for example), for $X \geq K \geq X^{\epsilon}$, we have

after shifting the integral to the $\frac{1}{2} - \sigma$ line and using $|\zeta(\sigma + it)| \ll t^{1/6}$ for $\sigma \geq \frac{1}{2}$. We write $J(s)$ for the integral in (20).

We have

$$\int_I |M(s)|^2 \, (K^{-1} + (1 + |s|)^{-1} + T^{-5/6})^2 \, |ds| \ll X^{-\phi}$$

by an easy calculation using (10). Also, using the fourth power moment of $\zeta(s)$ (see Chapter 7 of [13], for example) we have

$$\int_I |J(s)M(s)|^2 \, |ds| \ll \lambda \left(\frac{T}{K^2}\right)^{\frac{1}{2}} \left(1 + \frac{T}{M^2}\right)^{\frac{1}{2}} \ll X^{-\phi} .$$

This completes the proof of (19).

5. Estimation of Σ_1, Σ_2, Σ_3

(I) The main terms. We first note the forms which the functions $f(u)$ and $F(u)$ take for the present choice of parameters. We have, for $4 \leq u \leq 6$

$$f(u) = \frac{2\,e^{\gamma}}{u} \left(\log(u - 1) + \int_2^{u-2} \frac{\log(t - 1)}{t} \log\left(\frac{u - 1}{t + 1}\right) dt \right) .$$

In the case of Σ_1 $u = 105/26$, so

$$f(u) > \frac{2\,e^{\gamma}}{105/26} \log\left(\frac{79}{26}\right) .$$

Also, for $3 \leq u \leq 5$,

$$F(u) = \frac{2\,e^{\gamma}}{u} \left(1 + \int_2^{u-1} \frac{\log(t - 1)}{t} \, dt\right).$$

In the case of Σ_2 $u < 3$, and here $F(u) = 2\,e^{\gamma}/u$. For Σ_3 u varies, but it is never more than $52/17$. Thus in this case we have

$$F(u) \leq \frac{2\,e^{\gamma}}{u} \left(1 + \int_2^{35/17} \frac{\log(t-1)}{t} \, dt\right)$$

if

$$(MK)^{2+\tau} > T_1^4 X^{\varepsilon} . \tag{18}$$

Now, for $\beta = 8$, (18) follows from the hypothesis $KM \geq T_1^{6/7} X^{\varepsilon}$. Otherwise we use the definition of β to obtain

$$(MK)^{2+\tau} > X^{\varepsilon} T_1^{\theta(\beta)}$$

where

$$\theta(\beta) = 4\left(\frac{\beta-1}{\beta-2}\right)\left(\frac{10}{9} - \frac{4}{8+\beta}\right) \quad \text{for} \quad 8 < \beta < 10$$

$$= \frac{8}{9}\left(5 - \frac{4}{\beta-2}\right) \qquad \text{for} \quad \beta \geq 10 .$$

It may easily be verified that $\theta(\beta) \geq 4$ for all $\beta > 8$. It follows that (18) holds, and so the result of the lemma follows from (15), (16), (17).

We require one more lemma on mean values of Dirichlet polynomials.

LEMMA 6 *For* $K > T^{1/2}X^{\varepsilon}$, $KM > X^{1-\varepsilon}$, $T_0 \gg X^{\varepsilon/10}$, *we have*

$$\int_I |M(s)K(s)|^2 \, |ds| \ll X^{-\phi} . \tag{19}$$

Proof By the well known Perron formula (Lemma 3.12 of [13]), we have

$$K(s) = \frac{1}{2\pi i}\int_{c-iT-\sigma}^{c+iT-\sigma} \zeta(s+w)\,\frac{K^w(2^w-1)}{w}\,dw$$

$$+ O(K^{-1} + \frac{\log X}{T})$$

$$= \frac{1}{2\pi i}\int_{\frac{1}{2}-iT-\sigma}^{\frac{1}{2}+iT-\sigma} \zeta(s+w)\,\frac{K^w(2^w-1)}{w}\,dw \tag{20}$$

$$+ O(K^{-1} + T^{-5/6} + (|s|+1)^{-1}) ,$$

$$\leqslant \frac{2\,e^{\gamma}}{u}\left(1 + \int_2^{35/17} 1 - 2/t \;dt\right) = 2\,e^{\gamma}u^{-1}\,(1 + (1/17 - 2\log(35/34))$$

In the following we write $E^{\pm} = \pm C\varepsilon + O((\log X)^{-1/3})$, keeping to our convention that the C s need not be the same at each occurrence. By (6) the main term from Σ_1 is thus

$$\geqslant \frac{2\,y}{\log X} \log(79/26)\;(1 + E^{-}).$$

To estimate the main terms for Σ_2 and Σ_3 we use the following trivial inequality in order to simplify the estimation of the remainder terms :

$$\sum_{P \leqslant p < 2P} S(A_p, z_j(p)) \leqslant \frac{1}{\log P} \sum_{P \leqslant n < 2P} \Lambda(n)\, S(A_n, z_j(P)) \qquad (j = 3,4).$$

Thus the main term from Σ_2 using (2), (5) and the formula for F(u) is

$$\leqslant \sum_{z_2 \leqslant n < (2X)^{\frac{1}{2}}} \frac{2\,y\Lambda(n)\;(1 + E^{+})}{(\log n)\; n\; (\log(X/n))}$$

$$= 2\int_{9/35}^{1/2} \frac{dt}{t\,(1-t)}\;(1 + E^{+})\,\frac{y}{\log X}$$

$$= \frac{y}{\log X}\; 2\log(26/9)\;(1 + E^{+}).$$

Similarly, the main term from Σ_3 is

$$\leqslant \frac{y}{\log X}\; 2\log\left(\frac{79\times 27}{78\times 26}\right)\;(1 + (1/17 - 2\log(35/34))\,(1 + E^{+}).$$

Hence the main term from $\Sigma_1 - \Sigma_2 - \Sigma_3$ is

$$\geq \frac{-2y}{\log X} \log\left(\frac{79 \times 27}{78 \times 26}\right) (1/17 - 2\log(35/34))(1 + E^{+})$$

$$> -10^{-4}\, y/(\log X),$$

assuming ε is sufficiently small and X sufficiently large.

II The remainder terms. We wish to show that

$$\frac{1}{X}\int_{X}^{2X} R_{(D)}^{\pm 2}\, dx \ll Y^2 X^{-\phi}.$$

After a division of $R_{(D)}^{\pm}$ into $\ll \lambda$ subsums (note that the number of sequences (D) is $\ll 1$), this reduces to obtaining the same estimate for

$$\frac{1}{X}\int_{X}^{2X} |R_{(D)}^{-}(H, P_1;\ldots,P_r)|^2\, dx \quad \text{and} \quad \frac{1}{X}\int_{X}^{2X} |R_{(D)}^{+}(P,H,P_1,\ldots,P_r)|^2\, dx .$$

We now appeal to Lemma 3 , Corollaries (1) and (2), to reduce our task to obtaining the upper bound $X^{-\phi}$ for the integrals which occur on the right in (8) and (9).

We first consider Σ_1. If (D) is the empty sequence or has only 1 or 2 members then Lemma 6 may be applied since $P_1P_2 \leq (X^{26/105})^2 + 3\varepsilon < X^{\frac{1}{2}}$. This lemma gives the desired result whenever $H P_1 \ldots P_r < X^{11/20}$, so we henceforth suppose this condition is violated. If $r \geq 4$ then $P_r^6 < X$, so Lemma 5 may be applied $\ll 1$ times with $K(s)$ as a subsum of $L(s)$, $M(s)$ as a subsum of $H^{-}(s)\, P_1(s) \ldots P_{r-1}(s)$ and $N(s)$ as $P_r(s)$. For a sequence consisting of three members Lemma 5 may be applied if $P_3 < X^{8/35}$ or $H > X^{\varepsilon^2}$. Otherwise we note that P_1, P_2, P_3 are all greater than $T_1^{1/4}$, while $L > X^{1 - 2\varepsilon^2/z_1^3} > T_1^{2/7} X^{\varepsilon/10}$ (z_1 was chosen so that this last condition would hold). An appeal to Hölder's inequality, Lemma 4 Corollary and (10) completes the proof in this case.

For Σ_2 the empty subsequence may be dealt with simply by appealing to Lemma 6 since $P \ll X^{\frac{1}{2}}$. If a sequence has one member then at least one of $PD_1 < X^{11/20}$, $D_1 < X^{8/35}$ holds, for otherwise we would have $PD_1^3 > X$, which is impossible. For a sequence with r members where $r \geq 3$ we note that $D_r^6 < X$ so Lemma 5 is applicable. The remaining case of $r = 2$ is a little more troublesome. We may assume

$$P_2 > X^{8/35}, \quad X/(P P_1 P_2) < X^{9/35},$$

for otherwise the proof may be completed as for Σ_1' with $r = 3$. We note that we must have $P < X^{16/35}$ since $P_2 > X^{8/35}$. In this final case we must split $P(s)$ by Vaughan's identity (see [14]) into $\ll \lambda$ double sums of the form

$$\sum_{M<m\leq 2M} a_m \sum_{P\leq mn<Q} b_n (mn)^{-s}, \tag{23}$$

where either:

1) $P\, X^{-\varepsilon^2} \geq M \geq X^{\varepsilon^2}$,

or

2) $M < X^{\varepsilon^2}$ and $b_n \equiv 1$ or $\equiv \log n$.

In both cases

$$\sum_{M<m\leq 2M} a_m^k \ll \lambda M, \quad \sum_{N<n\leq N} b_n^k \ll \lambda N$$

and $a_m, b_n \ll X^{\eta}$ for any $\eta > 0$.

We now write

$$Q_1(s) = \sum_{M<m\leq 2M} a_m m^{-s}, \quad Q_2(s) = \sum_{\frac{P}{4M}<n<\frac{2P}{M}} b_n n^{-s} \tag{24}$$

Then the sum (23) may be expressed in the form

$$\frac{1}{2\pi i}\int_{-iT}^{iT} \left(\frac{Q^w - P^w}{w}\right) Q_1(s+w)\, Q_2(s+w)\, dw + (X^{\varepsilon} T^{-1}), \tag{25}$$

using the Perron formula and assuming, without loss of generality, that $\| P \| = \| Q \| = \frac{1}{4}$.

6. Estimating P_3s in the interval

We write

$$\psi(a) = \sum_{n \leq a} \Lambda(n) .$$

The following lemma gives the asymptotic formula for estimating subsums of Σ_4. The author first proved the result of this paper using the method of [3] in order to establish a lemma of the following type. Lemma 7 here is stronger and the proof is simpler, though for very short interval lengths the zero density method of [3] appears to be stronger.

LEMMA 7 Suppose $X^{1-\varepsilon} > PR \geq X^{27/35}$. Write

$$S = \sum_{P \leq n < 2P} \sum_{R \leq r < 2R} \Lambda(n)\Lambda(r) \left(\psi\left(\frac{x}{nr}\right) - \psi\left(\frac{x-y}{nr}\right) \right) .$$

Then we have

$$S = \sum_{P \leq n < 2P} \sum_{R \leq r < 2R} \left(\frac{\Lambda(n)\Lambda(r)}{nr}\right) y + E_1 + E_2 \qquad (28)$$

where

$$\frac{1}{X} \int_X^{2X} |E_j|^j \, dx \ll Y^j (\log X)^{-10} \quad (j = 1,2).$$

Proof. Our starting point will be the familiar formula, which follows from lemma 3.12 of [13]:

$$\sum_{A < n \leq qA} \Lambda(n) n^{-s} = -\frac{1}{2\pi i} \int_{c-\sigma-iT}^{c-\sigma+iT} \frac{\zeta'}{\zeta}(s+w) \frac{A^w(q^w - 1)}{w} dw + O\left\{ \frac{A^{1-\sigma}(\log A)^2}{T} + \frac{\log A}{A^\sigma} \right\}$$

(29)

Now, if we denote by $Q_3(s)$ a double sum of the form (23), we have, by (25)

$$\int_I |H^+(s)\, P_1(s)\, Q_3(s)\, P_2(s)\, L(s)\,|^2 |ds| \tag{26}$$

$$\ll \lambda \int_{-T}^{T} \frac{dt}{1+|t|} \int_I |H^+(s)\, L(s)\, Q_1(s+it) Q_2(s+it) P_1(s)\, P_2(s)\,|^2\, |ds|$$

$$+ O(X^{-\phi}).$$

It is easily demonstrated, using (13), that, for any value of t, the portion of the inner integral on the right of (26) corresponding to $|s+ti| \leq T^{\frac{1}{2}}$ is $\ll X^{-\phi}$. It thus suffices to prove that

$$\int_{s\in I,\ |s+it|>T^{\frac{1}{2}}} |H^+(s)\, Q_1(s+it)\, Q_2(s+it)\, P_1(s)\, P_2(s)|^2 |ds| \ll X^{-\phi} \tag{27}$$

for any t with $|t| \leq T$. If $Q_3(s)$ is a type 1) sum then

$$X^{\varepsilon^2} \leq \min(M,\ P/M) \leq P^{\frac{1}{2}} \leq X^{8/35}.$$

In this case Lemma 5 may be applied. For a sum of type 2) we note that $P/M \gg X^{9/35 - \varepsilon^2} > T_1^{2/7}\, X^{\varepsilon/10}$. The proof may then be completed as in other cases by Holder's inequality and Lemma 4 Corollary (with slight modifications to allow for $K(s)$ having the different form $Q_2(s+it)$). The motivation in the choice for z_2 is now clear.

We shall be brief in our discussion of Σ_3. The only sequence to give any trouble is, as with Σ_2, $r = 2$, $H < X^{\varepsilon^2}$, $P_2 > X^{8/35}$. In this case, however, $X/(PP_1P_2) > X^{1-2\varepsilon^2} / (P\,(z_4(P))^2) \gg X^{9/35 - 2\varepsilon^2} > T^{2/7}\, X^{\varepsilon/10}$. The proof may then be completed as for Σ_1 and Σ_2. The reason for the choice of $z_4(p)$ is now obvious.

Now we suppose $A >> T^{\varepsilon}$, then, using the zero free region of $\zeta(s)$ (see Corollary 11.4 of [11], for example) we may shift the integral in (29) to

$$\operatorname{Re} w = 1 - (\log A)^{-\frac{3}{4}} - \sigma$$

and only encounter the pole at $s + w = 1$, while on the new line of integration

$$\frac{\zeta'}{\zeta}(s) << (\log A)^3 .$$

The "horizontal" parts of the contour are

$$<< A^{c-\sigma} (\log A)^3 T^{-1} .$$

We thus find that

$$\sum_{A \leq n < 9A} \Lambda(n) n^{-s} = \frac{A^{1-s}(9^{1-s} - 1)}{1 - s}$$

$$+ O(A^{1-\sigma} \exp(-(\log A)^{\frac{1}{4}}) (\log A)^4).$$

We write

$$P(s) = \sum_{P \leq n < 2P} \Lambda(n) n^{-s}$$

and define $R(s)$ similarly. We also put $Q = (X - Y)/(4PR)$,

$$Q(s) = \sum_{Q \leq n \leq 9Q} n^{-s} \Lambda(n) .$$

Then

$$S = \frac{-1}{2\pi i} \int_{c-iT}^{c+iT} P(s)\,Q(s)\,R(s)\,\frac{(x-y)^s - x^s}{s}\,ds + O(YX^{-\phi}) + O(\epsilon_1)$$

from another application of Perron's formula. We write $B = \exp((\log P)^{1/5})$ and then

$$\frac{1}{2\pi i} \int_{c-iB}^{c+iB} P(s)\,Q(s)\,R(s)\,\frac{(x-y)^s - x^s}{s}\,ds$$

$$= \frac{1}{2\pi i} \int_{c-iB}^{c+iB} Q^{1-s}\frac{(q^{1-s}-1)}{1-s}\,P(s)R(s)\,\frac{(x-y)^s - x^s}{s}\,ds + O(Y(\log X)^{-10}). \tag{30}$$

Now

$$\frac{(x-y)^s - x^s}{s} = -yx^{s-1} + O(By^2 x^{c-2}).$$

The expression (30) thus becomes

$$\frac{y}{2\pi i} \int_{c-iB}^{c+iB} P(s)R(s)\,\frac{(x/Q)^{s-1}\,(1-q^{1-s})}{s-1}\,ds + O(Y(\log X)^{-10})$$

$$= y \sum_{P \le n < 2P} \sum_{R \le r < 2R} \frac{\Lambda(n)\Lambda(r)}{nr} + O(Y(\log X)^{-10})$$

using Perron's formula again. To complete the proof it thus suffices to show that

$$\int_{c+iB}^{c+iT} |P(s)\,Q(s)\,R(s)|^2\,|ds| \ll X(\log X)^{-10}. \qquad (31)$$

The inequality (31) may be proved in the same way as lemma 5 was demonstrated, using the present $Q(s)$ in the rôle played in lemma 5 by $K(s)$ since

$$Q(s) \ll B^{-1}$$

on the line of integration.

We are now in a position to give a lower bound for Σ_4. This sum counts all integers in $(x - y, x]$ of the form pqr where p,q,r are primes with

$$(X^{1-3\varepsilon}/p)^{1/3} \leq q < p < X^{\frac{1}{2}} \quad \text{and} \quad r \geq q, \quad p > X^{9/35}. \qquad (32)$$

We divide the sum into subsums $S(P,R)$ corresponding to $P \leq p < 2P$, $R \leq r < 2R$. Then

$$S(P,R) = \frac{(1+O((\log X)^{-1}))}{\log (X/PR)} \sum_{\substack{P \leq n < 2P \\ R \leq m < 2R}} \frac{\Lambda(n)\Lambda(m)}{\log P \log R} \left(\psi\left(\frac{x}{mn}\right) - \psi\left(\frac{x-y}{mn}\right)\right) + E_3$$

where

$$\frac{1}{X}\int_X^{2X} |E_3|\,dx \ll Y(P^{-1/3} + R^{-1/3} + (X/PR)^{-1/3}).$$

We may estimate $S(P,R)$ by Lemma 7 if $X^{1-\varepsilon} > PR \geq X^{27/35}$. If $64P^2R^3X^{1-3\varepsilon} \leq X^3$, $X^{9/35} \leq P \leq X^{\frac{1}{2}/2}$, and $PR \geq X^{27/35}$ then (33) holds ($r \geq q$ since $PR^2 = (PR)^2 P^{-1} > X^{54/35 - \frac{1}{2}} > X$) and $PR < X^{1-\varepsilon}$ so

$$\Sigma_4 \geq \frac{y}{\log X}\,(C_4 + O((\log X)^{-1})) + (\log X)^2(E_1 + E_2 + E_3).$$

Here

$$C_4 = \iint_{\frac{9}{35} \leq v \leq \frac{1}{2}} \frac{du\,dv}{uv(1-u-v)}\,,$$

$$u + v \geq \frac{27}{35}\,, \quad 2v + 3u \leq 2$$

The integral is estimated crudely as 27 times the area of integration and we find that

$$C_4 > 0.14.$$

8. Conclusion

Assembling all our information, we have shown, assuming ε is sufficiently small and X sufficiently large, that

$$\pi(x) - \pi(x-y) > y/(.8 \log x)$$

for all $x \in [X, 2X]$, except on a set of measure $< CX(\log X)^{-1}$. We note that $[x]$ takes on $\geq X - CX(\log X)^{-1}$ values, that

$$\pi([x]) - \pi([x] - y) > y(10 \log x)^{-1},$$

and $[x]^{(1/10)+\epsilon} \leq 2y \leq 2[x]^{(1/10)+\epsilon}$. This completes the proof of the theorem.

Possibly by using a more complicated decomposition instead of (3) one could estimate the remainder term in a satisfactory manner with an exponent smaller than 1/10.

By a similar method to that used in this paper, it will be shown elsewhere that there are infinitely many solutions of the inequality

$$\{\sqrt{p} - \beta\} < p^{-\frac{1}{4}+\epsilon}$$

for any real β. Here $\{x\}$ denotes the fractional part of x. The exponent $\frac{1}{4}$ improves on an exponent slightly smaller than 1/6 given by Kaufman [10].

Acknowledgements.

I would like to thank R.C. Baker for his careful checking of my manuscript and his helpful suggestions on matters of exposition. I would also like to thank R. Heath-Brown for an interesting discussion on the subject, and H. Iwaniec for his encouragement.

References

1. Cramér, H.: On the order of magnitudes of the difference between consecutive prime numbers. Acta Arith. 2, 23-46 (1937).

2. Halberstam, H., Richert, H.E.: Sieve Methods. London: Academic Press 1974.

3. Harman, G.: Almost-primes in short intervals. Math. Ann. 258 (1981)

4. Heath-Brown, D.R.: Zero density estimates for the Riemann Zeta-function and Dirichlet L-functions. J.London Math.Soc. (2), 19, 221-232 (1979).

5. Heath-Brown, D.R., Iwaniec, H.: On the difference between consecutive primes. Invent.Math. 55, 49-69 (1979).

6. Huxley, M.N.: On the difference between consecutive primes. Invent. Math. 15, 164-170 (1972).

7. Iwaniec, H.: A new form of the error term in the linear sieve. Acta Arith. 37, 307-320 (1980).

8. Iwaniec, H., Jutila, M.: Primes in short intervals. Ark. Mat. 17, 167-176 (1979).

9. Jutila, M.: Zero density estimates for L-functions. Acta Arith. 32, 55-62 (1977).

10. Kaufman, R.M.: The distribution of $\{\sqrt{p}\}$ (Russian). Math. Zam. 26, 497-504 (1979).

11. Montgomery, H.L.: Topics in multiplicative number theory. Berlin, Heidelberg, New York: Springer 1971.

12. Selberg, A.: On the normal density of primes in short intervals, and the difference between consecutive primes. Arch. Math. Naturvid. 47, 87-105 (1943).

13. Titchmarsh, E.C.: The Theory of the Riemann Zeta-function. Oxford 1951

14. Vaughan, R.C.: Sommes trigonometriques sur les nombres premiers. Comptes Rendus Acad. Sci. Paris, Serie A. 285, 981-983 (1977).

CHAPTER NINE

THE DISTRIBUTION OF $\sqrt{p}$ MODULO ONE

1. Introduction

It was shown by Vinogradov (see Theorem 7, Chapter 4 of [9]) that, for $\varepsilon > 0$, there are infinitely many solutions in primes p of the inequality

$$\{\sqrt{p}\} < p^{-\gamma+\varepsilon},$$

where $\{x\}$ denotes the fractional part of x and $\gamma = 0.1$. The value of γ was improved to

$$\frac{\sqrt{15}}{2(8+\sqrt{15})} = 0.1631006.....$$

by Kaufman [7]. On the Riemann Hypothesis he showed that one can take $\gamma = 1/4$. The method used actually shows that, for any real β and any α with $0 < \alpha < 1$, the number of primes $p \leq x$ satisfying

$$\{\sqrt{p} - \beta\} < \alpha$$

is

$$\alpha\, \pi(x) + O(x^{1-\gamma+\varepsilon} + \alpha x^{1-\varepsilon}). \qquad (1)$$

This may be restated in another form : the expression (1) represents the number of primes $p \leq x$ contained in intervals of the form

$$[(n+\beta)^2, (n+\beta)^2 + 2\alpha(n+\beta) + \alpha^2).$$

THEOREM. *For any* h *with* $0 \leq h \leq 1$ *and any* X, λ *write* $\pi^*(h, X, \lambda)$ *for the number of primes* p *with*

$$p \in [(n+h)^2, (n+h)^2 + n^{1-2\lambda})$$

for some n *with* $X^{\frac{1}{2}} \leq n \leq (2X)^{\frac{1}{2}}$. *Then, for* $\lambda < \frac{1}{4}$ *we have*

$$\pi^*(h, X, \lambda) > \frac{C(\lambda)\, X^{1-\lambda}}{\log X} \tag{2}$$

for $X > X_0(\lambda)$. *Here* $C(\lambda)$ *is a decreasing function of* λ *with* $C(\frac{1}{4}) > 0.18$.

COROLLARY. *For any real* β *there are infinitely many solutions of*

$$\{\sqrt{p} - \beta\} < p^{-\frac{1}{4}+\varepsilon}. \tag{3}$$

Remarks. As often occurs with a sieve method we are unable to give an asymptotic formula for the number of primes under consideration, but only a lower bound which is a fraction of the expected number (cf. [1], [2] and [5] for example). However, it is possible to use some of the methods of this paper to establish asymptotic formulae for a larger value of λ than that given by Kaufman. By working a little more carefully $n^{1-2\lambda}$ could be replaced by $n^{\frac{1}{2}} (\log n)^A$ for some sufficiently large constant A in (2). To simplify the proof we shall assume $h = 0$ and $\lambda = \frac{1}{4} - \varepsilon$ with ε "small". For the case $h \neq 0$ it is necessary to use the Hurwitz zeta function at certain stages of the proof. The only properties we require of this function, however, are its fourth power moment and its appearance in an analogue of lemma 3.12 of [8] (see (11) below - the well

This could be interpreted as an approximation to the conjecture that an irreducible quadratic polynomial with integer cofficients (the leading one being positive) takes prime values infinitely often. Sieve methods have enabled such conjectures to be solved with 'prime' replaced by 'almost-prime' (see, in particular, [6]). We shall use a sieve method here to prove the following result:

known Perron formula). Both these properties it shares with the Riemann zeta function.

2. Outline of the Method.

We work similarly to [1]. We use the standard notation

$$P(z) = \prod_{p<z} p, \quad V(z) = \prod_{p<z} (1 - 1/p) = \frac{e^{-\gamma}}{\log z}(1 + O((\log z)^{-1})).$$

For a finite set of integers A we write

$$A_d = \{n \in A;\ d|n\}$$

$$S(A,z) = |\{n \in A;\ (n, P(z))=1\}|.$$

The set A of interest to us with the present problem is

$$A = A(x) = \{m;\ x^2 < m \leq x^2 + y\}$$

with

$$y = x^2 (2X)^{-(\lambda+\frac{1}{2})}, \quad X \leq x^2 < 2X.$$

The fundamental Buchstab identity states that

$$S(A, z_1) = S(A, z_2) - \sum_{z_2 \leq p < z_1} S(A_p, p).$$

Using this we see that

$$\sum_{X \leq x^2 < 2X} (\pi(x^2 + y) - \pi(x^2)) \geq \sum_{X \leq x^2 < 2X} S(A, X^{\frac{1}{4}})$$

$$- \sum_{X \leq x^2 < 2X} \left(\sum_{X^{\frac{1}{4}} \leq p < X^{\frac{3}{8}}} S(A_p, p) + \sum_{X^{\frac{3}{8}} \leq p < X^{\frac{1}{2}}} S(A_p, z(p)) - \sum_{X^{\frac{3}{8}} \leq p < X^{\frac{1}{2}}} S(A_{pq}, q) \right)$$

$$z(p) \leq q < (\frac{X}{p})^{\frac{1}{2}}$$

$$= \sum_{X \leq x^2 < 2X} (\Sigma_1 - \Sigma_2 - \Sigma_3 + \Sigma_4) \quad \text{say.} \qquad (4)$$

In the above $z(p) = (X^{\frac{3}{4}}/p)^{\frac{1}{2}}$. By Σ'_j we shall mean the sum of the Σ_j over x.

We shall give a lower bound for Σ_1 and an upper bound for Σ_3 using the linear sieve with the error term in the form given by Iwaniec [5]. We give asymptotic formulae for Σ_2 and subsums of Σ_4 using similar methods to those used for estimating the remainder terms in the sieve. It should be noted that we do not need weighted zero density estimates (as in [2]) although we do require the zero free region of the Riemann zeta function (cf. [3]). The value $\frac{1}{4}$ is apparently the limit of every known method, so it is very interesting that, apart from the ε, this limit is reached. We now write

$$D = X^{1-2\eta}, \quad \eta = \varepsilon/20, \quad Y = X^{\frac{1}{2}-\lambda}, \quad T = X^{1+2\eta}Y^{-1}$$

for certain parameters which shall occur. We remark that the method may easily be extended to cover n^2 replaced by n^c for any $c > 1$ with $\frac{1}{4}$ replaced by $\lambda_o(c)$.

3. The Sieve result.

We write, for any set of integers B,

$$r(B,d) = |B_d| - |B|/d,$$

$$r(B_q,d) = |B_{qd}| - \frac{|B|}{qd}.$$

We shall use the linear sieve result of Iwaniec [4] in the form stated in [2]. When we come to apply lemma 1 the A and D occurring in its statement will not always be those specified in section 2. The properties of the standard functions $f(s)$ and $F(s)$ which occur

that are relevant here are

$$f(s) = \frac{2e^{\gamma}}{s} \log(s - 1) \qquad \text{for } 2 \leq s \leq 4 ,$$

$$F(s) = \frac{2e^{\gamma}}{s} \left(1 + \int_{2}^{s-1} \frac{\log(t - 1)}{t} \, dt\right) \qquad \text{for } 3 \leq s \leq 5 .$$

In the above γ is Euler's constant. In the following the letter C shall denote an absolute constant, not necessarily the same at each occurrence.

LEMMA 1. Let $z \geq 2$, $D \geq z^2$ and $\varepsilon > 0$. Then

$$S(A,z) \leq WV(z)\{F(s) + E\} + R^+ \tag{5}$$

$$S(A,z) \geq WV(z)\{f(s) - E\} - R^- \tag{6}$$

where $s = (\log D/(\log z)$ and $E = C\epsilon + O((\log D)^{-1/3})$. The remainder terms $R^{\pm}$ are of the form

$$R^{\pm} = \sum_{(D)} R^{\pm}_{(D)} = \sum_{(D)} \sum_{\nu < D^{\varepsilon}} C^{\pm}_{(D)}(\nu,\varepsilon) \sum'_{D_i \leq p_i \leq D_i^{1+\varepsilon^7}} r(A, \nu p_1 \ldots p_r) \tag{7}$$

where (D) runs over all subsequences $D_1 \geq D_2 \ldots \geq D_r$, including the empty subsequence, of the sequence

$$D^{\varepsilon^2(1+\varepsilon^7)^n}, \qquad n \geq 0,$$

for which

$$D_1 D_2 \ldots D_{2k} D_{2k+1}^3 \leq D \qquad (0 \leq k \leq (r-1)/2)$$

in the case of R^+, and

$$D_1 D_2 \ldots D_{2k-1} D_{2k}^3 \leq D \qquad (0 \leq k \leq r/2)$$

in the case of R^-. Moreover, Σ' indicates that ν and p_i, $(1 \leq i \leq r)$, are restricted by the conditions

$$\nu \mid P(D^{\varepsilon^2}), \quad p_i \mid P(z).$$

Finally, the coefficients $C^{\pm}_{(D)}(\nu,\varepsilon)$ depend at most on (D), ν, ε and the $\pm$ signs and satisfy

$$|C^{\pm}_{(D)}(\nu,\varepsilon)| \leq 1.$$

4. Some preliminary results

In this section we give the relation between the remainder terms and integrals of Dirichlet polynomials, and various estimates for such integrals. For any upper case latin letter B other than X, P, and H we write

$$B(s) = \sum_{B<b\leq 2B} \alpha_n b^{-s}$$

where α_n is real and $\sum_{B<b\leq 2B} \alpha_n^k \ll B^{1+\lambda}$, for any integer $k \leq C_1(\varepsilon)$.

For the letter L we stipulate other conditions. For

L, $\alpha_n = 1$ for some set of consecutive integers and $\alpha_n = 0$ otherwise. Also the condition $L < \ell \leq 2L$ is to be replaced by $C_2(\varepsilon) \leq \ell/L \leq C_3(\varepsilon)$.

For $1 \ll H \ll D^{\epsilon}$ we define $H^{\pm}(s)$ by

$$H^{\pm}(s) = \sum_{H\leq\nu<2H} C^{\pm}_{(D)}(\nu,\varepsilon)\, \nu^{-s}$$

For numbers P_j $(j = 1,\ldots r)$ with $D_j \leq P_j \leq D_j^{1+\varepsilon^7}$ we write

$$P_j(s) = \sum_{P_j\leq p_j<2P_j} p_j^{-s}\, \alpha^{(j)}_{p_j}$$

where $\alpha_n^{(j)} = 1$ for some set of consecutive integers n, and is zero otherwise.

We write $R(x^2; (D); P_1, \ldots, P_r)$ for that subsum of $R^{\pm}_{(D)}$ corresponding to $P_j \leq p_j < 2P_j$, and $R^{+}(x^2; P; (D), P_1, \ldots, P_r)$ for subsums of $R^{+}_{(D)}$ for Σ_3 with $P_j \leq p_j < 2P_j$ summed from $p = P$ to $2P - 1$. Here we are substituting A_p for A in (5) of course. The following lemma may be demonstrated in a similar manner to the corollaries of lemma 3 in [1].

LEMMA 2. (A) Write $L = X(H P_1 \ldots P_r)^{-1}$. Let A be as in section 2, and $z = X^{\frac{1}{4}}$. Then we have

$$R(x^2; (D); P_1, \ldots, P_r) = O(YX^{-\eta})$$

$$+ \frac{1}{2\pi i}\left(\int_{c-iT}^{c-iT_o} + \int_{c+iT_o}^{c+iT}\right) L(s)H^{-}(s)P_1(s)\ldots P_r(s)\,\frac{((x^2+y)^s - x^{2s})}{s}\,ds. \tag{8}$$

Here $c = 1 + (\log X)^{-1}$, $T_o = L^{-\frac{1}{2}}$.

(B) Write $L = X(H P P_1 \ldots P_r)^{-1}$. Replace A by A_p in (5) and D by D/P. Put $z = z(p)$. Then we have

$$R(x^2; (D); P, P_1, \ldots P_r) = O(YX^{-\eta})$$

$$+ \frac{1}{2\pi i}\left(\int_{c-iT}^{c-iT_o} + \int_{c+iT_o}^{c+iT}\right) L(s)H^{+}(s)P(s)P_1(s)\ldots P_r(s)\,\frac{(x^2+y)^s - x^{2s}}{s}\,ds. \tag{9}$$

We now give estimates for the type of integrals which occur in (8) and (9) which are also applicable (subject to slight modification) to the establishing of the asymptotic formulae in section 6. We write I for the line from $c + i\,T_o$ to $c + i\,T$. We also put

$$X(s) = \sum_{X^{\frac{1}{2}} \leq x < (2X)^{\frac{1}{2}}} x^{2s}$$

LEMMA 3. Suppose $X << M\,N << X$. Then, if $X^{\lambda + \varepsilon/2} \leq M < X^{\frac{3}{4} - \frac{3\lambda}{2} - \varepsilon/2}$,

$$\int_I |X(s)M(s)N(s)|\,|ds| << X^{\frac{3}{2} - \eta}. \tag{10}$$

Proof. We may suppose, without loss of generality, that $||X^{\frac{1}{2}}||$, $||(2X)^{\frac{1}{2}}|| > 10^{-3}$.

Then, by lemma 3.12 of [8], for $s = \sigma + it$,

$$X(s) = \frac{1}{2\pi i} \int_{2\sigma + c - Ti}^{2\sigma + c + Ti} \zeta(-2s + w)\, X^{w/2}\, \frac{(2^{w/2} - 1)}{w}\, dw + O\left(\frac{X^{\sigma + \frac{1}{2}} \log X}{T}\right) \tag{11}$$

$$= \frac{1}{2\pi i} \int_{-T}^{T} \zeta(\tfrac{1}{2} + i(u - 2t))\, X^{\frac{1}{4} + \sigma + iu/2}\, \frac{(2^{\frac{1}{4} + \sigma + iu/2} - 1)}{2\sigma + \frac{1}{2} + iu}\, du$$

$$+ O(X^{\sigma + \frac{1}{2}} \log X\, (1 + |t|)^{-1})$$

$$= X_1(s) + X_2(s).$$

Now we have

$$\int_I |X_2(s)M(s)N(s)|\,|ds| << \left(\int_I |M(s)N(s)|^2\,|ds|\right)^{\frac{1}{2}} \left(\int_{T_o}^{T} \frac{dt}{t^2}\right)^{\frac{1}{2}} (\log X) X^{\frac{3}{2}}$$

$$<< X^{3/2 - \eta},$$

$$L(s) = \frac{1}{2\pi i} \int_{\frac{1}{2} - c - iT}^{\frac{1}{2} - c + iT} \zeta(s + w)\, L^{w}\, \frac{(C_3^{w} - C_2^{w})}{w}\, dw$$

$$+ O(T^{-5/6} + L^{-1} + (1 + |s|)^{-1}).$$

It is easily seen, using $L > X^{\lambda + \varepsilon/2}$, that

$$\int_{c + iT_o}^{c + iT} |M(s)N(s)X_1(s)|\, (T^{-5/6} + L^{-1} + (1 + |s|)^{-1})|ds| \ll X^{\frac{3}{2} - \eta}.$$

An application of Holder's inequality to

$$\int_I \left| M(s)N(s)X_1(s) \int_{\frac{1}{2} - c - iT}^{\frac{1}{2} - c + iT} \zeta(s + w)\, L^{w}\, \frac{(C_2^{w} - C_3^{w})}{w}\, dw \right| |ds|$$

thus yields the bound

$$\left(\frac{T}{L^2}\right)^{\frac{1}{4}} \left(1 + \frac{T}{MN}\right)^{\frac{1}{2}} T^{\frac{1}{4}} X^{\frac{5}{4} + \eta} \ll X^{3/2 - \eta},$$

which completes the proof.

5. The estimation of Σ_1' and Σ_3'.

We write $E^{\pm} = \pm(C\eta + O(\log X)^{-1/3})$.

The main term for Σ_1' is

which is of the required size. Also, using Hölder's inequality and the well known result for the fourth power moment of $\zeta(s)$ (see [8], Chapter 13 for example) we arrive at the following inequality:

$$\int_I |X_1(s)M(s)N(s)|ds| \ll (1+T/M^2)^{\frac{1}{4}}(1+T/N)^{\frac{1}{2}} X^{5/4+\eta} T^{\frac{1}{4}} \ll X^{3/2-\eta}.$$

To obtain the final inequality we have used

$$\left(\frac{T}{M^2}\right)^{\frac{1}{4}} T^{\frac{1}{4}} = \frac{X^{\frac{1}{4}+\lambda/2+\eta}}{M^{\frac{1}{2}}} < X^{\frac{1}{4}+\eta-\varepsilon/4},$$

and

$$\frac{T^{\frac{3}{4}}}{N^{\frac{1}{2}}} = \frac{X^{\frac{3}{8}+3\lambda/4+3\eta/2}}{N^{\frac{1}{2}}} \ll M^{\frac{1}{2}} X^{\frac{3}{8}+3\lambda/4+3\eta/2-\frac{1}{2}}$$

$$\leq X^{\frac{3}{8}-3\lambda/4-\varepsilon/4+\frac{3}{8}+3\lambda/4+3\eta/2-\frac{1}{2}}$$

$$< X^{\frac{1}{4}-\eta}.$$

This completes the proof of the lemma.

LEMMA 4. Suppose $X \ll MNL \ll X$, $L > X^{\lambda+\varepsilon/2}$. Then

$$\int_I |X(s)L(s)M(s)N(s)| \, |ds| \ll X^{\frac{3}{2}-\eta}. \tag{12}$$

Proof. We work similarly to the previous lemma, but we apply the Perron formula to $L(s)$ as well as $X(s)$. The proof for $X_2(s)$ follows as before. We have

$$\frac{2\log 3}{\log X}(1+E^-) \sum_{X \leq x^2 < 2X} x^2 (2X)^{-(\lambda+\frac{1}{2})} = \frac{2\theta(\log 3)}{\log X} X^{1-\lambda}(1+E^-) \text{ say.}$$

The main term for Σ_3 is

$$\frac{2\theta X^{1-\lambda}}{\log X}\int_{\frac{3}{8}}^{\frac{1}{2}} \frac{d\alpha}{\alpha(1-\alpha)}\left(1+\int_2^{\frac{8(1-\alpha)}{3-4\alpha}-1}\frac{\log(t-1)}{t}\,dt\right)(1+E^+)$$

$$= \frac{2\theta X^{1-\lambda}}{\log X} C_4 (1+E^+) \text{ say.}$$

We now consider the remainder term for Σ_1'. We observe that

$$(x^2+y)^s - x^{2s} = x^{2s}((1+Y/X)^s - 1)$$

while $\frac{(1+Y/X)^s - 1}{s} \ll \frac{Y}{X}$. In view of (8) it thus suffices to show that the ranges of summation in a remainder term may be grouped together so that the hypotheses of lemmas 3 or 4 are satisfied. If there are no more than 3 P_j ranges then lemma 4 is applicable since

$$P_1P_2P_3 \leq D_1D_2D_3X^\eta \leq X^{2/3}D_1^{1/3} \leq X^{1-\lambda-\varepsilon}.$$

If there are four ranges and $P_1P_2P_3P_4 > X^{1-\lambda-\varepsilon}$ we note that

$$P_1P_2P_3P_4^3 < X, \text{ so } P_4 < X^{\frac{1}{8}}. \quad \text{Thus}$$

$$X^{1-\lambda-\varepsilon} > P_1P_2P_3 > X^{\frac{1}{4}+\frac{3\lambda}{2}+\varepsilon/2}$$

and so lemma 3 is applicable with $M(s) = H^-(s)L(s)P_4(s)$.

If there are five ranges and $P_1 .. P_s > X^{1-\lambda-\varepsilon}$ we note that lemma 3 may be applied if

$$X^{\frac{1}{4}+\frac{3\lambda}{2}+\frac{\varepsilon}{2}} < P_1 \dots P_4 \leq X^{1-\lambda-\varepsilon/2}$$

and the above argument for four ranges may be invoked once more if

$$P_1 .. P_4 > X^{1-\lambda-\varepsilon/2} .$$

We may thus assume that

$$P_1 \dots P_4 < X^{\frac{1}{4}+\frac{3\lambda}{2}+\varepsilon/2} .$$

In this case, however,

$$P_4P_5 \geq P_5^2 X^{-\eta} > X^{\frac{3}{2}-5\lambda-2\varepsilon-\eta} > X^{\lambda+\varepsilon/2}$$

while $P_4P_5 \leq X^{\eta} \min(P_3^2, (X/P_1P_2P_3)^{2/3}) \leq X^{\eta} \min(P_3^2, X^{\frac{2}{3}} P_3^{-2})$

$$\leq X^{1/3+\eta} < X^{\frac{3}{4}-3\lambda/2-\varepsilon} ,$$

so the hypotheses of lemma 3 are satisfied in this case as well. The proof for six or more ranges follows similarly.

We shall be brief in our discussion of Σ_3'. Because of our choice of $z(p)$ we find that

$$P P_1 P_2 < X^{1-\lambda-\varepsilon/2}$$

and so a remainder term with no more than two ranges of summation may be

estimated from lemma 4. A remainder term with r ranges $(r > 2)$ may be bounded in exactly the same way as the remainder term for Σ_1' with $r + 1$ ranges (note we did not use the fact that $P_1 \leq X^{\frac{1}{4}}$ in the discussion for Σ_1' for $r \geq 4$).

6. Asymptotic formulæ.

Our starting point will be the familiar formula, which follows from lemma 3.12 of [8]:

$$\sum_{A < n < 2A} \Lambda(n)n^{-s} = \frac{-1}{2\pi i}\int_{c-\sigma-iT}^{c-\sigma+iT} \frac{\zeta'}{\zeta}(s+w)\,\frac{A^w(2^w-1)}{w}\,dw \qquad (13)$$

$$+ O\left(\frac{A^{1-\sigma}(\log A)^2}{T} + \frac{(\log A)}{A^\sigma}\right).$$

Now we suppose $A >> T^\varepsilon$, then, using the zero free region of $\zeta(s)$ (see [7]) we may shift the integral in (13) to $\mathrm{Re}\, w = 1 - (\log A)^{-\frac{3}{4}} - \sigma$ and only encounter the pole at $s + w = 1$, while on the new line of integration $\zeta'/\zeta << (\log A)^3$. The "horizontal" parts of the contour are

$$<< A^{c-\sigma}(\log A)^3 T^{-1}.$$

We thus find that

$$\sum_{A < n < 2A} \Lambda(n)n^{-s} = \frac{A^{1-s}(2^{1-s}-1)}{1-s} + O(\exp(-(\log A)^{\frac{1}{4}})A^{1-\sigma}(\log A)^4)$$

We write

$$P_1(s) = \sum_{P_1 < n < 2P_1} \Lambda(n) n^{-s}$$

and define $P_2(s)$ similarly, but with the range of summation extended from $P_2/2$ to $4P_2$. Here $P_1 P_2 = X$.

Then

$$\sum_{P_1 < n < 2P_1} \sum_{m} \Lambda(n)\Lambda(m) = + \frac{1}{2\pi i} \int_{c-iT}^{c+iT} P_1(s) P_2(s) \frac{(x^2+y)^s - x^{2s}}{s} ds + O(YX^{-\eta})$$

$$x^2 < mn < x^2 + y$$

from another application of Perron's formula. We now write $B = \exp((\log X)^{1/5})$, then

$$\frac{1}{2\pi i} \int_{c-iB}^{c+iB} P_1(s) P_2(s) \frac{(x^2+y)^s - x^{2s}}{s} ds$$

$$= \frac{1}{2\pi i} \int_{c-iB}^{c+iB} \frac{P_1^{1-s}(2^{1-s} - 1)}{1-s} P_2(s) \frac{((x^2+y)^s - x^{2s})}{s} ds + O(Y(\log X)^{-10}). \quad (14)$$

Now $$\frac{(x^2+y)^s - x^{2s}}{s} = y\, x^{2(s-1)} + O(B y^2 x^{2c-4}).$$

The expression (14) thus becomes

$$\frac{y}{2\pi i} \int_{c-iB}^{c+iB} P_2(s) \frac{(x^2/P_1)^{s-1}(1 - 2^{1-s})}{s-1} ds + O(Y(\log X)^{-10})$$

$$= y \sum \frac{\Lambda(n)}{n} + O(Y(\log X)^{-10})$$

$$\frac{x^2}{2P_1} < n < \frac{x^2}{P_1}$$

using Perron's formula again. Thus we need only obtain the estimate

$$\int_{c+iB}^{c+iT} |P_1(s)P_2(s)X(s)| \, |ds| \ll X^{\frac{3}{2}}(\log X)^{-10}$$

in order to establish an asymptotic formula for P_2s, and similarly for P_3s etc. The proof of lemma 3 holds for the above type of integral since the only place where T_o was used occurs in the estimate of the integral involving $X_2(s)$. Since the estimate involved is actually

$$X^{\frac{3}{2}}(\log X)^C \, T_o^{-\frac{1}{2}}$$

for some C, we thus obtain the required estimate if

$$X^{\frac{1}{4}} \leq P_1 \leq X^{\frac{3}{8}}.$$

The asymptotic formula itself is

$$\Sigma_2' = \frac{\theta X^{1-\lambda}}{\log X} \left(\int_{\frac{1}{4}}^{\frac{3}{8}} \frac{d\alpha}{\alpha(1-\alpha)} + \int_{\frac{1}{4}}^{\frac{1}{3}} \int_{\alpha}^{\frac{1-\alpha}{2}} \frac{d\alpha \, d\beta}{\alpha(1-\alpha-\beta)\beta} \right) (1 + E^+)$$

$$= \frac{\theta X^{1-\lambda}}{\log X} (1 + E^+) C_5 \quad \text{say.}$$

Similarly we can establish an asymptotic formula for subsums of Σ_4

References

1. G. Harman, "Primes in short intervals", to appear.

2. D. R. Heath-Brown and H. Iwaniec, "On the difference between consecutive primes", Invent. Math. 55, 49-69 (1979).

3. D. R. Heath-Brown, "Prime numbers in short intervals and a generalized Vaughan identity", to appear.

4. H. Iwaniec, "A new form of the error term in the linear sieve". Acta Arithmetica 37, 307-320 (1980).

5. ————————, "Almost-primes represented by quadratic polynomials". Invent. Math. 47, 171-188 (1978).

6. R. M. Kaufman, "The distribution of $\{\sqrt{p}\}$" (Russian), Mat. Zam. 26 (1979) 497-504.

7. H. E. Richert, "Zur Abschätzung der Riemannschen zetafunktion in der Nähe der Vertikalen $\sigma = 1$", Math. Ann., 16 (1967), 97-101.

8. E. C. Titchmarsh, Theory of the Riemann zeta-function, Oxford 1951.

9. I. M. Vinogradov, Special variants of the method of trigonometric sums, Nauka, Moscow 1976.

corresponding to $X^{\frac{3}{8}} < p < X^{\frac{1}{2}}$, $X^{\frac{1}{4}} < q < (X/p)^{\frac{1}{2}}$. The term we get here is

$$\frac{\theta X^{1-\lambda}}{\log X}(1 + E^{-}) \int_{\frac{3}{8}}^{\frac{1}{2}} \int_{\frac{1}{4}}^{\frac{1-\alpha}{2}} \frac{d\alpha\, d\beta}{\alpha\beta(1-\alpha-\beta)}$$

$$= \frac{\theta X^{1-\lambda}(1 + E^{-1}) C_6}{\log X} \quad \text{say.}$$

7. Completion of the proof.

It now only remains to verify that

$$2 \log 3 - 2C_4 - C_5 + C_6 > 0 .$$

We have $2 \log 3 > 2.19$, while simple computation shows that

$$2C_4 < 1.15, \quad C_5 < 0.81, \quad C_6 > 0.10 .$$

We also have $\theta = \frac{2^{\frac{3}{2}} - 1}{3} > 0.6$, so $C(\frac{1}{4}) > 0.18$ as claimed.

CHAPTER TEN

ON THE DISTRIBUTION OF αp MODULO ONE

1. Introduction. In this paper we shall use a sieve method to prove the following result:

THEOREM 1. *Suppose that α is irrational and $\|\gamma\|$ denotes the distance of γ from a nearest integer. Then, for any real number β, there are infinitely many primes p such that*

$$\|\alpha p - \beta\| < p^{-3/10}. \tag{1}$$

The best known result of the above type which has previously appeared is due to R.C. Vaughan [7], who obtained $1/4$ in place of $3/10$ in (1), and who also required an additional factor $(\log p)^8$ on the right hand side of (1). D.R. Heath-Brown has obtained the exponent $4/15 = 0.266\ldots$ (private communication) using a sieve method. Earlier work on this problem was done by I.M. Vinogradov (see Chapter 11 of [8]) who obtained the exponent $1/5 - \epsilon$, essentially using the sieve of Eratosthenes. The elementary method introduced by Vaughan for dealing with sums over primes is no stronger than Vinogradov's method however, the improved result in [7] coming from a more careful application of the auxiliary results on trigonometric sums. It should be noted that we will use exactly the same trigonometric sum estimates as occur in [7]. We will also employ the linear sieve (see [5]) and the fundamental Buchstab identity (see (2) below). These last two tools enable us to avoid estimating certain "awkward" types of sums which arise in the work of Vinogradov and Vaughan. Because we discard these sums our present result is not quite so precise as theirs, for they establish an asymptotic formula, involving the denominators of the continued fraction

expansion of α, for the number of primes $p \leq X$ with $\|\alpha p - \beta\| < \delta$, whereas we can only obtain a lower bound. Of course this is a common feature of sieve results (see [4], for example).

It is possible to improve on the value 3/10 in (1), but, as should become apparent in the subsequent sections, the working becomes much clumsier as one increases this value, and one has to resort to numerical integration of a rather unwieldly nature. The present approach provides an alternative for certain problems to the methods of Vinogradov and Vaughan which, instead of breaking down at a certain point as one attempts to strengthen the result, changes smoothly from giving an asymptotic formula to giving a lower bound. The asymptotic formula has a much weaker error term than that given by the other methods however. Unfortunately the present method alone does not seem capable of giving improved results for the problem of the distribution of αp^k modulo one (for which see [1] and [3]), although it will lead to an enhanced outcome for certain other problems (for example one may ameliorate [4] using the present approach). By using the present approach in tandem with a more conventional use of the linear sieve, however, one can produce a slight improvement on the results on αp^k for $k \geq 3$. A rough outline is given in section 4. We also mention the following theorem which improves upon work of Graham [2] and follows immediately from Lemmas 2 and 3 below together with Theorem 4 of [5].

THEOREM 2 Let P_r denote a number with at most r prime factors ($r \geq 2$). Then, given the hypotheses of Theorem 1, there are infinitely many solutions of

$$\| \alpha P_r + \beta \| < P_r^{-1+ 2/(r+1)+\varepsilon} .$$

2. Notation and preliminary results.

Throughout this paper ρ shall denote a prime number.

Here we write

$$P(z) = \prod_{p<z} p .$$

In the following ε is to be considered as a fixed small positive number. Let τ be a number between $1/4$ and $1/3$, where ε is small in terms of $1 - 3\tau$, and let a/q be a convergent to the continued fraction for α. We put

$$X = q^{2/(1+\tau)}, \quad L = X^{\tau-\varepsilon/2}, \quad \delta = X^{-\tau+\varepsilon}, \quad \eta = \varepsilon/20,$$

$$B = \{n : X \leq n < 2X\},$$

$$A = \{n : n \in B, \| \alpha n - \beta \| < \delta\},$$

$$A_d = \{n : n \in A, d|n\} .$$

We also write

$$S(E,z) = \{n \in E, (n,P(z)) = 1\}$$

for any set of integers E and a positive number z. The fundamental Buchstab identity states that

$$S(E,z_1) = S(E,z_2) - \sum_{z_2 \leq p < z_1} S(E_p,p) . \qquad (2)$$

The rest of this section will be concerned with establishing certain

auxiliary results which will be combined to prove the following formula for as wide a choice of D and $z(d)$ as is possible:

$$\sum_{D\leq d<2D} a_d S(A_d, z(d)) = \sum_{D\leq d<2D} a_d S(B_d, z(d)) 2\delta(1+E), \tag{3}$$

Here a_d are numbers all of the same sign and E is an acceptable small error. We could then give an asymptotic formula for the right hand side of (3) using the prime number theorem. It will then only remain to use (2) to relate $S(A, (2X)^{\frac{1}{2}})$ to expressions such as occur on the left hand side of (3) with certain non-negative sums left over for which we cannot show that (3) holds. The proof is then completed by showing that not too many of these "awkward" sums occur.

Constants implied by the O notation may depend on ε and τ. We shall use θ to denote a constant, not necessarily the same at each occurence, bounded above and below by numbers independent of ε, τ and D.

LEMMA 1. *Let a_m be a sequence of reals for $X \leq M < 2X$, all of the same sign. Then we have*

$$\sum_{m\in A} a_m = 2\delta \sum_{X\leq m<2X} a_m + O\left(\sum_{\ell=1}^{L} \delta \left| \sum_{X\leq m<2X} a_m e(m\ell\alpha)\right|\right) + O\left(\frac{1}{L}\sum_{X\leq m<2X} a_m\right). \tag{4}$$

Proof. Write $\chi(x)$ for the characteristic function of $(-\delta,\delta)$ extended to be periodic with period 1. It follows from [6] that there exist two sequences $b_-(k)$, $b_+(k)$ such that

$$\sum_{k=-L}^{L} b_-(k)\, e(xk) \leq \chi(x) \leq \sum_{k=-L}^{L} b_+(k)\, e(kx)$$

where $b_{\pm}(0) = 2\delta \pm (L+1)^{-1}$

and $b_{\pm}(k) \ll \delta$ for $k \neq 0$.

The proof of (4) follows easily since

$$\sum_{m\in A} a_m = \sum_{X\leq m<2X} a_m \chi(m\alpha - \beta) .$$

LEMMA 2. Suppose a_d all have the same sign and $a_d \ll X^{\eta}$. Then

$$\sum_{d<D} a_d|A_d| = 2\delta \sum_{d<D} a_d \frac{X}{d} + O\left(\sum_{\ell=1}^{L} \delta \left| \sum_{d<D} a_d \sum_{X<md\leq 2X} e(md\ell\alpha)\right|\right)$$

$$+ O(X^{1-\eta}\delta)$$

for $D \leq X^{1-\varepsilon}$.

Proof This easily follows from Lemma 1 upon noting that

$$\sum_{d<D} a_d|A_d| = \sum_{r\in A} \Big(\sum_{\substack{d<D\\ d|r}} a_d\Big) ,$$

$$\sum_{X\leq r<X} \sum_{\substack{d|r\\ d<D}} a_d f(r) = \sum_{d<D} a_d \sum_{X\leq md<2X} f(md) ,$$

and

$$\sum_{X\leq md<2X} 1 = \frac{X}{d} + O(1) .$$

LEMMA 3. Suppose that $b_n \ll X^{\eta}$. Then we have

$$\sum_{R \leqq \ell < 2R} \Big| \sum_{N \leqq n < 2N} b_n \sum_{X \leqq mn < 2X} e(\alpha nm\ell) \Big| \ll (XRq^{-1} + RN + q)X^{2\eta} . \tag{5}$$

Proof. This is essentially Lemma 3 of [7]. We shall require bounds for sums that occur on the right hand side of (5) which are $O(X^{1-\eta})$. Lemma 3 thus furnishes us with a satisfactory estimate when $N \leqq X^{1-\tau}$.

LEMMA 4. Suppose that $a_n, b_m \ll X^{\eta}$. Then we have

$$\sum_{R \leqq \ell < 2R} \Big| \sum_{N \leqq n < 2N} a_n \sum_{X \leqq mn < 2X} b_m e(\alpha nm\ell) \Big| \tag{6}$$

$$\ll XR(q^{-\frac{1}{2}} + (q/XR)^{\frac{1}{2}} + \min((X/N)^{-\frac{1}{2}} + (RN)^{-\frac{1}{2}}, (XR/N)^{-\frac{1}{2}} + N^{-\frac{1}{2}}))\, X^{3\eta}.$$

Proof. This follows from Lemma 2 of [7]. The estimate given by (6) is of a suitable size providing

$$X^{\tau} \leqq N \leqq X^{1-2\tau} \quad \text{or} \quad X^{2\tau} \leqq N \leqq X^{1-\tau} .$$

It is now clear that problems will arise with sums where one range is between $X^{1-2\tau}$ and X^{τ}, and it is these which we seek to avoid. The following lemma incorporates our use of the sieve and provides the first version of (3). This result effectively "sifts out" numbers from A which have a lot of small prime factors.

LEMMA 5 Suppose $M \leq X^{2\tau}$. Then, for $b_m \ll X^{\eta}$

$$\sum_{M\leq m<2M} b_m S(A_m,X^{\varepsilon}) = \sum_{M\leq m<2M} b_m S(B_m,X^{\varepsilon})\, 2\delta(1+E), \tag{7}$$

where

$$E = \theta\,\varepsilon^3 + O((\log X)^{-1/3}) + \theta\, e^{-(1-3\tau)/\varepsilon}.$$

Proof We write

$$r(A_m,d) = \frac{A}{md} - |A_{md}|\ .$$

We do not require the new form of the error term in the linear sieve for the proof of our result, but we refer the reader to [5] for the sake of convenience. We have (Theorem 4 of [5] replacing ε there by ε^3), for certain sequences $a_d^{\pm}$ with $a_d^{\pm} = O(1)$, that

$$S(A_m,X^{\varepsilon}) \leq \left(\frac{e^{-\gamma}}{\varepsilon \log X}\right)\left(\frac{2\delta X}{m}\right)(F(s)+E^{+}) + O\left(\sum_{d<\frac{X^{1-\tau}}{M}} a_d^{+}\, r(A_m,d)\right)$$

while

$$S(A_m,X^{\varepsilon}) \geq \frac{e^{-\gamma}\, 2\delta X}{(\varepsilon \log X)\, m}(f(s)+E^{-}) + O\left(\sum_{d<\frac{X^{1-\tau}}{M}} a_d^{-}\, r(A_m,d)\right),$$

where $s = \dfrac{\log(X^{1-\tau}/M)}{\varepsilon \log X} > \dfrac{1-3\tau}{\varepsilon}$,

$$E^{\pm} = O((\log X)^{-1/3}) \pm |\theta|\,\varepsilon^3,$$

and

$$F(s) - f(s) < |\theta| e^{-s} \leq |\theta| e^{(1-3\tau)/\varepsilon}.$$

We also have

$$S(B_m, X^{\varepsilon}) = \frac{e^{-\gamma}}{\varepsilon \log X} \frac{X}{M}(1 + E)$$

It therefore only remains to show that

$$\sum_{M \leq m < 2M} \Big| b_m \sum_{d < \frac{X^{1-\tau}}{M}} a_d \, r(A_m, d) \Big| \ll X^{1-2\eta} \delta. \tag{8}$$

(We assume here that the right hand side of (7) is $\gg X^{1-\eta}\delta$, this in fact always holds in our applications). The bound (8) is, however, a simple consequence of Lemmas 2 and 3.

The following is another version of (3).

LEMMA 6. *Suppose that* $X^{\tau} \leq M \leq X^{1-2\tau}$ *or* $X^{2\tau} \leq M \leq X^{1-\tau}$. *Also let* $c_r = 0$ *for* $r < X^{\varepsilon}$, *and suppose* $a_m, b_n, c_r \ll X^{?}$. *Then*

$$\sum_{M \leq m r < 2M} a_m c_r \sum_{N \leq n < 2N} b_n \, S(A_{mnr}, r) = 2\delta \sum_{M \leq m r < 2M} a_m c_r \sum_{N \leq n < 2N} b_n \, S(B_{mnr}, r)(1 + E)$$

whenever the right hand side above is $> X^{1-\eta}\delta$.

Proof. This follows from Lemmas 1 and 4.

We are now in a position to prove our main version of (3).

LEMMA 7. *Suppose that* $M \leq X^{1-\tau}$, $a_m \ll x^{\eta}$. *Then we have*

$$\sum_{M \leq m < 2M} a_m \, S(A_m, X^{1-3\tau}) = \sum_{M \leq m < 2M} 2\delta \, a_m \, S(B_m, X^{1-3\tau})(1 + E) \tag{9}$$

whenever the right hand side of (9) *is* $\gg X^{1-\eta}\delta$. *Here*

$$E = \theta\varepsilon + O((\log X)^{-1/3}) + \theta\varepsilon^{-2} e^{-(1-3\tau)/\varepsilon}.$$

Proof If $M \geq X^{2\tau}$ this follows from Lemma 6 so we may suppose that $M < X^{2\tau}$. By (2) we have

$$\sum_{M<m<2M} a_m S(A_m, X^{1-3\tau}) = \sum_{M\leq m<2M} a_m S(A_m, X^{\varepsilon}) \tag{10}$$

$$- \sum_{M\leq m<2M} \sum_{X^{\varepsilon}\leq p<X^{1-3\tau}} S(A_{mp},p) .$$

For the first sum on the right of (10) we may apply Lemma 5. We apply Lemma 6 to any subsum of the second sum with $pM \geq X^{2\tau}$ (since $p < X^{1-3\tau}$ we have $pM < X^{1-\tau}$). We then apply the Buchstab identity again to the remaining part of the subsum:

$$\sum_{M\leq m<2M} a_m \sum_{X^{\varepsilon}\leq p<X^{2\tau}/M} S(A_{mp},p) = \sum_m a_m \sum_p S(A_{mp}, X^{\varepsilon}) \tag{11}$$
$$p<X^{1-3\tau}$$

$$- \sum_m a_m \sum_p \sum_{X^{\varepsilon}<r<p} S(A_{mpr},r) .$$

(The ranges of summation over m and p on the right of (11) are the same as on the left). Lemma 5 may be applied to the first sum on the right of (11) and Lemma 6 may be used for any subsum of the second with $rpM \geq X^{2\tau}$. We continue this procedure, which must cease after $< \varepsilon^{-1}$ operations, until we have decomposed our original sum into parts for each of which we have given a formula of type (3). Clearly, upon combining all the sums of the type which occur on the right of (3) (reversing the decomposition), we obtain the right hand side of (9).

3. Proof of Theorem 1. In the following q,r,s are prime variables of summation, q no longer appears as the denominator of the convergent to the conintued fraction for α. We write $\sigma = X^{1-3\tau}$, $\rho = X^{\tau}$, $\mu = X^{1-2\tau}$, $\nu = (2X)^{\frac{1}{2}}$. We make one primary decomposition of $S(A,\nu)$ using (2) in the following way:

$$S(A,\nu) = S(A,\sigma) - \sum_{\sigma \leqq p < \rho} S(A_p,\sigma) - \sum_{\rho \leqq p \leqq \mu} S(A_p,p) - \sum_{\mu < p < \nu} S(A_p,\sigma)$$

$$+ \sum_{\sigma \leqq q < p < \rho} S(A_{pq},q) + \sum_{\substack{\mu < p < \nu \\ \sigma \leqq q \leqq (2X/p)^{\frac{1}{2}}}} S(A_{pq},q) .$$

$$= \Sigma_A - \Sigma_B - \Sigma_C - \Sigma_D + \Sigma_E + \Sigma_F, \text{ say} \qquad (12)$$

We remark that the upper bound for q in Σ_F is $(2X/p)^{\frac{1}{2}}$ and not p since the sum is clearly empty for $q > (2X/p)^{\frac{1}{2}}$, and this value is always less than p in Σ_F. By Lemma 6 and 7 we can give a formula of type (3) for the first four sums in (12). Also, we can immediately give such formulae for subsums of Σ_E where $\rho \leqq pq \leqq \mu$ and of Σ_F where $X/\mu < pq \leqq X/\rho$. This gives an overall lower bound for $S(A,\nu)$ of

$$\frac{2\delta X}{\log X}\left(1 - \frac{\log X}{X} \sum_{p,q} S(B_{pq},q)\right), \qquad (13)$$

where the summation in (13) is over those ranges of p and q for which we cannot show that (3) holds. We have omitted from (13) certain terms which either tend to zero with decreasing ε or increasing X such as $\theta\varepsilon^{-2}\, e^{-(1-3\tau)/\varepsilon}$ or $O((\log X)^{-1/3})$. This is legitimate provided we show that the term in brackets in (13) is bounded below by

$$\sum_{Y < p < Z} f(p) \leq (1 + \varepsilon^2) \int_Y^Z \frac{f(u)du}{\log u} \tag{16}$$

for a "well-behaved" non-negative function f.

Now, for Σ_E if $pq < \rho$ then $pq^2 < X/\rho$ so we can decompose this part of the sum further as in (14). The sum we are left with is

$$\sum_{\substack{\sigma \leq p < \sigma^2 \\ \sigma \leq s < r < q < \min(p, \rho/p)}} S(A_{pqrs}, s) . \tag{17}$$

We can give a type (3) formula for subsums of (17) with $qsr \leq \mu$ or $pqr \leq \mu$. The relevant term in (13) corresponding to the remainder of (17) is thus

$$\frac{\log X}{X} \sum_{\substack{\sigma \leq p < \sigma^2 \\ \sigma \leq s < r < q < \min(p, \rho/p) \\ qsr > \mu}} S(B_{pqr}, s) \leq (1 + \varepsilon) \int_R \frac{dudvdwdx}{uvwx^2}$$

$$< 0.016.$$

In the above R is the four dimensional region bounded by the inequalities $2/15 < u < 1/6$, $2/15 < v < \min(u, 3/10 - u)$, $2/5 - u - v < w < v$, $2/5 - v - w < x < w$. The numerical value was obtained by replacing R with the larger region $2/15 < u < 1/6$, $1/8 < w < 3/20$, $2/15 < v < 3/20$, $1/10 < x < 3/20$ and then elementary integration gives the value

$$\frac{10}{3} \ell n \left(\frac{6}{5}\right) \ell n \left(\frac{5}{4}\right) \ell n \left(\frac{9}{8}\right).$$

All integrals will be estimated in this elementary manner, so we shall be more brief with the details in future.

a constant independent of ε and X. The bound (13) may be improved by noting that we can decompose $S(A_{pq},q)$ further if $pq^2 < X/\rho$:

$$S(A_{pq},q) = S(A_{pq},\sigma) - \sum_{\sigma \leq r < q} S(A_{pqr},\sigma) + \sum_{\sigma \leq \sigma < r < q} S(A_{pqrs},s). \tag{14}$$

The condition $pq^2 < X/\rho$ is necessary for the second sum on the right of (14), which with the first term may then be estimated by Lemma 7. The contribution from the "awkward" part of the final sum is smaller than $S(A_{pq},q)$ and so we have made a saving.

Another way of improving (13) comes from considering what numbers are counted by $S(A_{pq},q)$ for the remaining ranges of p and q. Clearly we cannot find a formula of the required type for the primes counted, but possibly for some or all almost-primes we could find such a formula. The term $S(B_{pq},q)$ in (13) could then be replaced by a function which only counted the numbers for which we could not give a formula. Eventually, working as efficiently as is possible, we get a lower bound $2\delta XC(\tau)$, and it would be desirable to find the largest value of τ for which $C(\tau) > 0$. A moment's thought reveals that $C(\tau)$ is a continuous decreasing function of τ with $C(\frac{1}{4}) = 1$. To prove our theorem we need only show that $C(3/10) > a > 0$, where a is independent of X and ε. It then follows that $C(3/10 + \varepsilon) > a' > 0$ for some a' which is also independent of X and ε.

In fact, for $\tau = 3/10$ we do not need to work in a particularly efficient manner to obtain a positive lower bound. We will use the rather crude inequality

$$S(B_n, z) \leq \frac{X(1 + \varepsilon^2)}{n \log z} \tag{15}$$

several times in the following. We shall also employ the prime number theorem combined with partial summation in the form

The rest of Σ_E is split into two parts. In one $X^{7/30} < p < X^{3/10}$, $(X^{7/10}/p)^{\frac{1}{2}} < q < p$. For this part we can give no further decomposition. We find that the contribution to (13) from this subsum is

$$\frac{\log X}{X} \sum_{p,q} S(B_{pq},q) \leqq (1+\varepsilon) \int_{7/30}^{3/10} \int_{7/20 - \frac{u}{2}}^{u} \frac{dudv}{uv^2}$$

$$< 0.207 .$$

In the other part $X^{1/5} < p < X^{3/10}$, $X^{2/5}/p < q < \min(p,(X^{7/10}/p)^{\frac{1}{2}})$, so we may decompose the sum further. The "left-over" sum is

$$\sum_{\substack{X^{1/5} < p < X^{3/10} \\ X^{2/5}/p < q < \min(p,(X^{7/10}/p)^{\frac{1}{2}}) \\ X^{1/10} < s < r < q}} S(A_{pqrs},s) \qquad (18)$$

We can give a type (3) formula for most of (18). The remaining part has $pqr < X^{3/5}$, $qr < X^{3/10}$, $X^{7/10}/(pqr) < s < r$, $qsr > X^{2/5}$. The corresponding four dimensional integral is < 0.100.

We may now turn our attention to what remains of Σ_F. The part with $X^{2/5} < p < (2X)^{\frac{1}{2}}$, $X^{7/10} < pq < (2X\,p)^{\frac{1}{2}}$ cannot be decomposed further. This gives a contribution

$$(1+\varepsilon) \int_{2/5}^{\frac{1}{2}} \int_{\frac{7}{10}-u}^{\frac{1-u}{2}} \frac{dudv}{uv^2} < 0.088.$$

In the final part of Σ_F we have $pq < X^{3/5}$. If $q > (X^{7/10}/p)^{\frac{1}{2}}$

we are unable to perform a further decomposition. This gives rise to a term

$$(1+\varepsilon)\int_{2/5}^{\frac{1}{2}}\int_{\frac{7}{20}-\frac{u}{2}}^{3/5-u}\frac{dudv}{uv^2} < 0.269.$$

For $q < (X^{7/10}/p)^{\frac{1}{2}}$ the remaining sum after decomposition is

$$\sum_{X^{2/5} < p \leq (2X)^{\frac{1}{2}}} S(A_{pqrs},s)$$

$$X^{1/10} \leq s < r < q < (X^{7/10}/p)^{\frac{1}{2}}$$

Now, we can give a formula of type (3) for this if $qrs < X^{2/5}$. This always holds if $(X^{7/10}/p)^{3/2} < X^{2/5}$, i.e. if $p > X^{13/30}$. The remaining contribution is thus

$$(1+\varepsilon)\int_{2/5}^{13/30}\int_{2/15}^{7/20-u/2}\int_{\frac{1}{5}-\frac{v}{2}}^{v}\int_{\frac{2}{5}-w-v}^{w}\frac{du\,dv\,dw\,dx}{uvwx^2} < 0.006.$$

Combining all the above results we have

$$C(3/10) > 1 - (0.016 + 0.207 + 0.1 + 0.088 + 0.269 + 0.006) = 0.314.$$

This completes the proof of the theorem.

4. A note on αp^k. Here we shall briefly sketch the proof to the following result.

THEOREM 3. Given the hypotheses of Theorem 1 and an integer $k \geq 3$, there are infinitely many primes p such that

$$\| \alpha p^k - \beta \| < p^{-\xi+\varepsilon}$$

where

$$\xi = \frac{k}{(2k+1)(2^k-1)} .$$

The value of ξ improves upon

$$\frac{k}{2(k+1)(2^k-1)+1}$$

given in [3].

We put $A = \{n: n \in B , \| \alpha n^k - \beta \| < X^{-\xi+\varepsilon}\}$,

$$\lambda = \frac{\xi(2^{k+1} - 1)}{2k} = \frac{2^{k+1} - 1}{2(2k+1)(2^k-1)} \quad \text{and} \quad \tau = \frac{1}{2k + 1} .$$

By the trigonometric sum estimates given in [3] we may estimate the sums which will occur of the form

$$\sum_{\ell = 1}^{L} \Big| \sum_{N \leq n < 2N} a_n \sum_{X \leq mn < 2X} b_m \, e(\alpha m^k n^k \ell) \Big|$$

providing $X^{k\tau} \leq N \leq X^{1-k\tau}$, $X^{2\xi} \leq N \leq X^{\frac{1}{2}-\lambda}$ or

$X^{\frac{1}{2}+\lambda} \leq N \leq X^{1-2\xi}$. Furthermore, if $b_m \equiv 1$ we may obtain a suitable bound if $N \leq X^{k\tau}$. The basic decomposition we employ is

$$S(A,(2X)^{\frac{1}{2}}) = S(A,X^{\frac{1}{2}-\lambda}) - \sum_{X^{\frac{1}{2}-\lambda} \leq p < X^{k\tau}} S(A_p, X^{\tau}) - \sum_{X^{k\tau} \leq p < (2X)^{\frac{1}{2}}} S(A_p, p).$$

$$+ \sum_{\substack{X^{\frac{1}{2}-\lambda} \leq p < X^{k\tau} \\ X^{\tau} \leq q < (2X/p)^{\frac{1}{2}}}} S(A_{pq}, q)$$

$$= \Sigma_1 - \Sigma_2 - \Sigma_3 + \Sigma_4 \quad \text{say.}$$

For Σ_1 we can give an asymptotic formula working similarly to Lemma 7. We can also give such a formula for Σ_3. For Σ_2 we may use the linear sieve (here we do require the new form of the error term) to give an upper bound. Finally we are able to give an aymptotic formula for much of Σ_4 and we discard what remains. A simple numerical calculation then completes the proof. It should be noted that the limit of the method is not set here by the point where the final constant becomes zero, but by the difficulty in estimating Σ_2.

References

1. A. Ghosh, "The distribution of αp^2 modulo one", Proc. London Math. Soc. (3) 42 (1981) 252-269.

2. S.W. Graham, "Diophantine approximation by almost-primes", to appear.

3. G. Harman, "Trigonometric sums over primes II", Glasgow Math. Journal, to appear.

4. G. Harman, "Primes in short intervals", to appear.

5. H. Iwaniec, "A new form of the error term in the linear sieve", Acta Arithmetica. 37(1980) 307-320.

6. H.L. Montgomery, "The analytic principle of the large sieve", Bull. Am. Math. Soc. 84(1978), 547-567.

7. R.C. Vaughan, "On the distribution of αp modulo 1", Mathematika 24 (1977), 135-141.

8. I.M. Vinogradov, The method of trigonometric sums in the theory of numbers, (translated from the Russian by K.F. Roth and A. Davenport) Wiley-Interscience 1954.

R.J. Cook, "On the fractional parts of an additive form", Proc. Camb. Phil. Soc. 72 (1972), 209-212.

J.G. Van der Corput and Ch. Pisot, "Sur la discrepance Modulo un I & II", Proc. Kon. Ned. Ated. v. Wetensch. Amsterdam, 42 (1939), 476 - 485 & 554 - 565.

H. Cramer, "On the order of magnitude of the difference between consecutive prime numbers", Acta Arith. 2 (1937), 23 - 46.

N. Cudakov, "On Goldbach - Vinogradov's theorem", Ann. Math. 48 (1947), 515 - 545.

I. Danicic, Ph.D. Thesis London 1957.

----------, "An extension of a theorem of Heilbronn", Mathematika 5 (1958), 30 - 37.

----------, "On the fractional parts of βx^2 and ϕx^2", J. London Math. Soc. 34 (1959), 353 - 357.

H. Davenport, "Indefinite quadratic forms in many variables (II)", Proc. London Math. Soc. (3) 8 (1958), 109 - 126.

----------, "Analytic methods for diophantine equations and diophantine inequalities", Lecture notes, Univ. of Michigan, 1962.

----------, "On a theorem of Heilbronn", Quart. J. Math. Oxford (2), 18 (1967), 339 - 344.

----------, Multiplicative Number theory, second edition, Springer - Verlag, New York 1980.

H. Davenport & H. Heilbronn, "On indefinite quadratic forms in five variables", J. London Math. Soc. 21 (1946) 185 - 193.

H. Davenport & D. Ridout, "Indefinite quadratic forms", Proc. London Math. Soc. 9 (1959), 544 - 555.

H. Davenport & K.F. Roth, "The solubility of certain diophantine inequalities", Mathematika 2 (1955) 81 - 96.

H. Davenport & W.M. Schmidt, "Dirichlet's Theorem on diophantine Approximation, "Acta Arithmetica XVl (1970) 413 - 424.

COMPLETE REFERENCES.

A. Baker, "On some Diophantine Inequalities involving the exponential function". Can. J. Math. 17 (1963), 616-627.

R.C. Baker, "Recent results on fractional parts of polynomials", Number Theory Carbondale 1979, 10-19, Lecture Notes in Mathematics No.751, Springer, Berlin.

----------, "Fractional parts of several polynomials III", Quart. Journal Math. Oxford (2), 31 (1980)., 19-36.

----------, "Small fractional parts of the sequence αn^k," Michigan Mathematical Journal, 28 (1981)

----------, "Weyl sums and Diophantine Approximation", J. London Math. Soc. (2), 25 (1982), 25-39.

R.C. Baker and G. Harman, "Small fractional parts of Quadratic Forms", J. Edinburgh Math. Soc.

----------, "Small fractional parts of Quadratic and Additive Forms", Math. Proc. Camb. Phil. Soc. 90 (1981) 5-12.

----------, "Small fractional parts of polynomials", Proceedings of the Colloquium on Number Theory. Budapest 1981, To appear.

----------, "Diophantine approximation by prime numbers", J. London Math. Soc.

H. Behnke, "Zur Theorie der diophantische Approximation I", Abh. Math. Sem. Hamburg 3, 261-318 (1924).

J.W.S. Cassels, An introduction to Diophantine Approximation, Cambridge Tracts in Math. and Math. Physics, No. 45 (1957)

Chen, Jing-Run, "Estimates for trigonometric sums", Chinese Mathematics 1965 vol. 6, 163-167.

--------, "On the representation of a large even integer as the sum of a prime and the product of at most two primes"

Sci. Sinica 16 (1973), 157-176.

A. Ghosh, "The distribution of αp^2 modulo one", Proc. London Math. Soc. (3) 42 (1981) 252-269.

S.W. Graham, "Diophantine approximation by almost-primes" (unpublished).

H. Halberstam & H.E. Richert, Sieve Methods, London, Academic Press 1974.

G.H. Hardy & J.E. Littlewood, "Some problems of diophantine approximation", Acta Math. 37 (1914) 155-191.

----------, "On Partitio Numerorum I", Gottinger Nachrichter, 1920, 33-54.

G.H. Hardy & E.M. Wright, An introduction to the theory of numbers, Oxford, fifth edition 1979.

G. Harman, "Almost-primes in short intervals", Math. Ann. 258, 107-112 (1981).

----------, "Trigonometric Sums over primes I", Mathematika, 28 (1981), 249-254.

----------, "Trigonometric sums over primes II", Glasgow Math.J.

----------, "Primes in short intervals", Math, Zeit.

----------, "The distribution of $\sqrt{p}$ modulo one".

----------, "On the distribution of αp modulo one" J. London Math. Soc. to appear.

D.R. Heath-Brown, "Almost primes in arithmetic progressions and short intervals", Math. Proc. Camb. Phil. Soc. 83 (1978) 359-395.

----------, "The fourth power moment of the Riemann zeta function", Proc. London Math. Soc. (3) 38 (1979) 385-422.

----------, "Zero density estimates for the Riemann zeta function and Dirichlet L - functions" J.London Math. Soc.(2) 19 (1979) 221-232.

----------, "Prime numbers in short intervals and a generalized Vaughan identity", to appear.

D.R. Heath-Brown & H. Iwaniec, "On the difference between consecutive primes", Invent. Math. 55, 49-69 (1979)

H. Heilbronn, "On the distribution of the sequence $n^2\theta$ (Mod 1)", Quart. J. Math. Oxford (1), 19 (1945), 249-256.

G. Hoheisel,"Primzahlprobleme in der Analysis", Sitz Preuss. Akad. Wiss., 33 (1930). 3-11.

C. Hooley, "On a new technique and its applications to the theory of numbers", Proc. London Math. Soc. (3) 38 (1979). 115-151.

L.K. Hua, Additive prime number theory, Amer. Math. Soc. Trans., Vol. 13, Providence, R.I., 1965.

M.N. Huxley, "On the difference between consecutive primes", Invent. Math. 15, 164-170 (1972).

A.E. Ingham, "Mean value theorems in the theory of the Riemann zeta function," Proc. London Math. Soc (2) 27 (1926) 273-300.

----------, "On the difference between consecutive primes", Quart. J. Math. Oxford, 8 (1937), 255-266.

H. Iwaniec, "Almost-primes represented by quadratic polynomials", Invent. Math. 47 (1978), 171 - 188.

----------, "A new form of the error term in the linear sieve", Acta Arithmetica 37 (1980) 307-320.

H. Iwaniec & M. Jutila, "Primes in short intervals", Ark. Mat.17, 167-176 (1979).

D.L. Jagerman, "The auto correlation and joint distribution function of the sequences $\{(a/m)j^2\}$, $\{(a/m)(j+\tau)^2\}$ "; Math. Comp. 18 (1964) 211-232.

M. Jutila, "Zero density estimates for L-functions", Acta. Arith. 32, 55-62 (1977).

R.M. Kaufman, "The distribution of $\{\sqrt{p}\}$ " (Russian), Mat. Zam. 26 (1979) 497 - 504.

N.M. Korobov, "Estimates for trigonometric sums and their applications" (Russian), Uspehi Mat. Nauk (13) (1958) 82, 185-192.

L. Kuipers & H. Niederreiter, Uniform distribution of sequences, Wiley - Interscience New York 1974.

M.C. Liu, "On the fractional parts of θn^k and ϕn^k", Quart. J. Math. Oxford (2), 21 (1970), 481-486.

---------, "Recent developments of some analogues of Waring's problem and Dirichlet's theorem involving primes", Southeast Asian Bull. Math. 3 (1979) 193-202.

H.L. Montgomery, Topics in multiplicative number theory, Springer-Verlag Berlin 1971.

----------, "The analytic principle of the large sieve", Bull. Amer. Math. Soc. 84 (1978), 547-567.

Y. Motohashi, "A note on almost-primes in short intervals", Proc. Japan Acad. Ser. A. Math. Sci 55 (1979), 225-226.

K. Ramachandra, "On the sums $\Sigma \lambda_j f_j(\rho_j)$ ", J. Reine Angew. Math. 262/263 (1973), 158-165.

H.E. Richert, "Zur Abschatzung der Riemannschen zeta funktion in der Nahe der Vertikalen $\sigma = 1$", Math. Ann., 16(1967), 97-101.

A. Schinzel, H.P. Schlickewei & W.M. Schmidt, "Small solutions of quadratic congruences and small fractional parts of quadratic forms", Acta Arithmetica 37 (1980) 241-248.

H.-P. Schlickewei, "On indefinite diagonal forms in many variables", J. Reine Angew. Math. 307/8 (1979), 279-294.

W.M. Schmidt, "Simultaneous approximation to algebraic numbers by rationals", Acta Math. 125 (1970), 189-201.

----------, "Two questions in Diophantine Approximation", Monatshefte für Mathematik 82 (1976), 237-245.

----------, "On the estimation of a trigonometric sum over primes", ibid. 12 (1948) 225-248.

----------, The method of trigonometric sums in the theory of numbers, English trans. 1954, Wiley New York 1954, Russian revised edition 1971 Nauka, Moscow.

----------, Special variants of the method of trigonometric sums, Nauka, Moscow 1976.

A. Walfisz, Weylsche exponential Summen in der neuren Zahlentheorie. Berlin, Deutscher Verlag der Wiss, 1963.

G.L. Watson, "On indefinite quadratic forms in five variables", Proc. London Math. Soc. (3) 3(1953) 170-181.

H. Weyl, "Uber die Gleichverteilung von Zahlen mod Eins", Math. Ann. 77, 313-352 (1916).

D. Wolke, " Fast-Primzahlen in Kurzen Intervallen", Math. Ann. 244, 233-242 (1979).

----------, Small fractional parts of polynomials, Amer. Math Soc. Providence R.I. 1977.

----------, "Small zeros of additive forms in many variables", Trans. Amer. Math. Soc. 248 (1979), 121-133.

----------, "Diophantine inequalities for forms of odd degree", Advances in Math. 38 (1980), 128-151.

W. Schwarz, "Uber die Losbarkeit gewisser Ungleichungen durch primzahlen", J. Reine Angew. Math. 212 (1963) 150-157.

A. Selberg, "On the normal density of primes in short intervals, and the difference between consecutive primes", Arch. Math. Naturvid. 47, 87-105 (1943).

E.C. Titchmarsh, The theory of the Riemann Zeta-function Oxford 1951.

R.C. Vaughan, "Diophantine approximation by prime numbers I & II" Proc. London Math. Soc. (3) 28 (1974) 373 - 384 & 385 - 401.

----------, "Mean value theorems in prime number theory", J.London Math. Soc. (2) 10, (1975) 153-162.

----------, "Sommes trigonometriques sur les nombres premiers", C.R. Acad. Sci. Paris, Serie A 285, 981-983 (1977).

----------, "On the distribution of αp modulo one", Mathematika 24, 48 (1977) 136-141.

----------, "An elementary method in prime number theory", Acta Arithmetica, 37 (1980), 111-115.

I.M. Vinogradov, "On the fractional parts of integral polynomials", (Russian), Izv. Akad. Nauk. SSSR 20, 585-600.

----------, "A new estimate of a trigonometric sum containing primes", ibid. Ser. Mat. 2 (1938) 1-13.

----------, "On the estimation of some simplest trigonometric sums containing primes", ibid. 2. (1939), 371-395.