COLLOQUIA MATHEMATICA
SOCIETATIS JÁNOS BOLYAI, 51

NUMBER THEORY
Vol. I.
Elementary and Analytic

Edited by

K. GYŐRY and G. HALÁSZ

NORTH-HOLLAND

COLLOQUIA MATHEMATICA
SOCIETATIS JÁNOS BOLYAI, 51

NUMBER THEORY

Vol. I.

Elementary and Analytic

Edited by

K. GYŐRY and G. HALÁSZ



NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM – OXFORD – NEW YORK

© BOLYAI JÁNOS MATEMATIKAI TÁRSULAT

Budapest, Hungary, 1990

ISBN North-Holland: 0444 70476 0 VOL. I. – II.
0444 70346 2 VOL. I.

ISBN Bolyai: 963 8022 42 6 VOL. I. – II.
963 8022 45 0 VOL. I.

ISSN Bolyai: 0 139 3383 Hibás szám

ISSN 0139-3383

Joint edition published by

JÁNOS BOLYAI MATHEMATICAL SOCIETY

and

ELSEVIER SCIENCE PUBLISHERS B. V.

Saraburgerhartstraat 25, P. O. Box 103

1000 AC, Amsterdam, The Netherlands

In the U.S.A. and Canada:

ELSEVIER SCIENCE PUBLISHING COMPANY INC.

655 Avenue of Americas

New York, N. Y. 10010

U.S.A.

Assistant editor: A. BALOG and J. PINTZ

R 2

Printed in Hungary
Franklin Nyomda
Budapest

MC109747/1

SZÉCHENYI KÖNYVTÁR

1990

CONTENTS

Volume I.

	Page
PREFACE	7
J. DIXMIER and J.-L. NICOLAS, Partitions without small parts	9
P.D.T.A. ELLIOTT, Applications of elementary functional analysis to the study of arithmetic functions	35
P. ERDŐS and A. IVIĆ, The distribution of values of a certain class of arithmetic functions at consecutive integers	45
P. ERDŐS and M. SZALAY, On some problems of the statistical theory of partitions	93
J. FEHÉR, On real-valued R-additive functions	111
G. FREIMAN, A. HEPPES and B. UHRIN, A lower estimation for the cardinality of finite difference sets in R^n	125
A FUJII, Uniform distribution of the zeros of the Riemann zeta function and the mean value theorems	141
D.R. HEATH-BROWN, Sums of three square-full numbers	163
M.N. HUXLEY and N.WATT, The Hardy-Littlewood method for exponential sums	173
K.-H. INDLEKOFER, Limit laws and moments of additive functions in short intervals	193
M. JUTILA, The fourth power moment of the Riemann zeta-function over a short interval	221
J. KACZOROWSKI, A note on the non-trivial zeros of Dirichlet L-functions	245
I. KOREC, On number of cosets in non-natural disjoint covering systems.	265
E. MANSTAVIČIUS, Laws of the iterated logarithm for additive functions	279
F. MARKO, The sum of absolute values of coefficients of some Artin L-functions associated with rational characters.	301
Ch. MAUDUIT, Substitutive normal sets	317
T. MEURMAN, On the order of the Maass L-function on the ciritical line	325

Page

B. MOSSÉ, q-adic spectral analysis of arithmetic sequences 355

K. NAGASAKA, S. KANEMITSU and J.-S. SHIUE, Benford's law: The logarithmic law of first digit . . . 361

M. NAIR and A. PERELLI, On the distribution of $p^{1/2}$ modulo one 393

M.B. NATHANSON, Extremal properties for bases in additive number theory 437

C. POMERANCE and A. SÁRKÖZY, On products of sequences of integers 447

H. PORTA and K.B. STOLARSKY, The edge of a golden semigroup 465

I. Z. RUZSA, Arithmetical topology 473

I. SHIOKAWA, Asymptotic distributions of digits in integers 505

G. SZEKERES, Asymptotic distribution of partitions by number and size of parts 527

S.T. TULYAGANOV, On the summation of multiplicative arithmetical functions 539

Volume II.

	Page
E. BAYER-FLUCKIGER, Week Hasse principle for systems of bilinear forms	581
B. BRINDZA, Power values of sums $1^k+2^k+\ldots+x^k$ . . .	595
M. DENERT, Type number and class number of hereditary orders in non Eichler (R)-algebras of prime index over global function fields. .	613
R. DVORNICICH and C. VIOLA, Some remarks on Beuker's integrals	637
G.R. EVEREST, The S-unit equation and Dirichlet series	659
J.H. EVERTSE and K. GYŐRY, On the number of solutions of unit equations and decomposable polynomial equations	671
G. FOLZ and H.G. ZIMMER, A boundedness theorem for the torsion of elliptic curves over algebraic number fields	697
A. GEROLDINGER, On non-unique factorisations into irreducible elements II	723
W. JEHNE, Presentations of Weil groups and global skew fields	759
P. KISS, On primitive prime power divisors of Lucas numbers	773
K. LAKKIS, Special product relations between local Gauss sums	787
E. LAMPRECHT, Integral bases in function and number fields	795
V. LAOHAKOSOL, J.H. LOXTON and A.J. van der POORTEN, Integer-valued p-adic functions. . .	829
F. LORENZ, Normal bases of units	851
R.A. MOLLIN, An overview of the solution to the class number one problem for real quadratic fields of Richaud-Degert type	871
T. NAKAHARA, A construction of quadratic fields whose class numbers are divisible by a power of 3	889
A. PETHŐ, Divisibility properties of linear recursive sequences	899
A. ROTKIEWICZ and W. ZŁOTKOWSKI, On the diophantine equation $1+p^{\alpha 1}+p^{\alpha 2}+\ldots+p^{\alpha k}=y^2$ . .	917

Page

J. RUTKOWSKI, A p-adic analogue of the Legendre system 939

H. P. SCHLICKEWEI and W. M. SCHMIDT, Bounds for zeros of quadratic forms 951

W. M. SCHMIDT, The number of solutions of norm form equations 965

R. TIJDEMAN, The number of solutions of diophantine equations 979

N. TZANAKIS, On the practical solution of the Thue equation, an outline 1003

M. WALDSCHMIDT, Dependence of logarithms of algebraic points 1013

B. M. M. de WEGER, On the practical solution of Thue-Mahler equations, an outline 1037

J. WOLFART, Values of Gauss' continued fractions . . 1051

LIST OF PARTICIPANTS 1065

Preface

Continuing a tradition, the János Bolyai Mathematical Society held a conference on number theory in Budapest from the 20th to the 25th July, 1987. There were 138 participants from 22 countries, 24 of them from Hungary. The need to make room for over 90 talks forced us to divide into two parallel sections, one on the elementary and analytic and one on the diophantine and algebraic theory. We organized 10 common lectures making a point of inviting mostly young people as speakers. These lectures were to make a bridge between the two sections, not with full success, though. (In order to maintain the more intimate atmosphere of the earlier meetings we have decided to hold two smaller meetings in the future corresponding, by and large, to the above division of the field.)

The present volumes contain most, though not all, of the papers presented at the conference; in few cases the published papers differ from the ones read. They vary from short summaries to self-contained articles with full proofs. Their topics include elementary number theory, sequences of integers, additive and multiplicative number theory, exponential and character sums, zeta and L-functions, uniform distribution, diophantine approximation, geometry of numbers, transcendental numbers, polynomials, finite fields, algebraic number theory, arithmetic algebraic geometry and computational number theory.

We thank the participants for the successful conference and the rich volumes.

Budapest, 1989.

The Organizing Committee

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

PARTITIONS WITHOUT SMALL PARTS

DIXMIER, J. and NICOLAS, J.-L.*

1. INTRODUCTION

Let us denote by $p(n)$ the number of non restricted partitions of n. It is known from Hardy and Ramanujan (cf. [Ram], §36 and [Rad], p. 278) that:

$$(1) \qquad p(n) = \frac{1}{2\pi\sqrt{2}} \frac{d}{dn} \frac{\exp(C\sqrt{n - 1/24})}{\sqrt{n - 1/24}} + f_1(n)$$

where the constant C is equal to $\pi\sqrt{2/3} = 2.565...$ and:

$$(2) \qquad f_1(n) = O\left(\frac{1}{n} \exp \frac{C\sqrt{n}}{2}\right) .$$

---

* Research partially supported by Centre National de la Recherche Scientifique: Greco "Calcul formel" and PRC "Math-Info".

In [Nic], it is proved that $|f_1(n)| \leq \frac{1}{n} \exp\left(\frac{C\sqrt{n}}{2}\right)$ for $n > 26$. Actually, looking at the values of $f_1(n)$ for $1 \leq n \leq 25$, this inequality holds for all $n \geq 1$. With more accurate estimations, it can be shown that $|f_1(n)| \leq \frac{0.11..}{n} \exp\left(\frac{C\sqrt{n}}{2}\right)$, for all $n \geq 1$, with equality for $n = 12$. Let us set:

$$(3) \qquad g(\lambda,t) = \left(\exp\left(C\,\frac{\sqrt{1-\lambda t^2}-1}{t}\right)\right)\left(C(1-\lambda t^2)^{-1} - t(1-\lambda t^2)^{-3/2}\right).$$

Expanding the derivative, formula (1) writes:

$$(4) \qquad p(n) = \frac{\exp(C\sqrt{n})}{4\pi\sqrt{2}n}\; g(1/24,\ 1/\sqrt{n}) + f_1(n).$$

The function $g(\lambda,t)$, with λ fixed, is analytic at $t = 0$. Using its Taylor expansion, we can get an asymptotic expansion of $p(n)$ according to powers of $1/\sqrt{n}$. In particular:

$$(5) \qquad p(n) = \frac{\exp(C\sqrt{n})}{4\sqrt{3}n}\,(1 + O(1/\sqrt{n})).$$

Now, we define $p(n,m)$ as the number of partitions of n whose parts are $\leq m$; or, what is equivalent, as the number of partitions of n in at most m parts.

Finally, we define $r(n,m)$ as the number of partitions of n whose parts are $\geq m$. These notations are borrowed from the Gupta-Gwyther-Miller tables (cf. [Gup 1]); these tables give the formulas:

$$r(n,m) = r(n,m+1) + r(n-m,m); \quad r(n,n) = 1.$$

These formulas were used by Gupta (cf. [Gup 4]) to calculate by hand the values of $r(n,m)$ and of $p(n) = r(n,1)$ for $n \leq 300$. Let us mention also:

$$(6) \qquad r(n,m) = \sum_{t=0}^{\lfloor n/m \rfloor} p(n - tm, t) \quad ([Gup\ 1],\ p.xi\ i\ i)$$

and it is easy to see that:

$$(7) \qquad r(n,m) \leq p(n, \lfloor n/m \rfloor).$$

By definition, $\lfloor x \rfloor = \max_{n \in \mathbb{Z}, n \leq x} n$

Using (6), Gupta, in [Gup 2], gave an asymptotic estimate of $r(n,m)$, valid for $n = O(m \log m)$.

Recently, J. Herzog gave in his thesis (cf. [Her], p. 57) the following estimate, valid for $m = O(n^{3/8} (\log n)^{3/4})$:

$$\log r(n,m) = C\sqrt{n} - \frac{1}{2} m \log n + m \log m - m\left(1 + \log \frac{\sqrt{6}}{\pi}\right) +$$

$$+ O(n^{1/4} \sqrt{\log n}).$$

This result is obtained by using a Tauberian theorem.

On the other hand, Erdős and Szalay studied the analogous problem for unequal partitions. Let $q(n)$ be the number of unequal partitions of n, and $\rho(n,m)$ the number of unequal partitions of n whose parts are $\geq m$; they proved (cf. [Erd 2], p. 433) that, for $m \leq n^{1/5}$,

$$\rho(n,m) = (1 + o(1))\, q(n)/2^{m-1}$$

by integrating the generating function in the complex domain.

A more complicate asymptotic estimation of $\rho(n,m)$ has been given in [Erd 3], which is valid for $m \leq n^{3/8-\varepsilon}$

Finally, in [Odl], A. Odlyzko has studied $\Delta^k(p(n))$ where Δ^k is the kth forward difference operator, with a method somewhat similar to that one which we shall use below. We shall prove:

THEOREM 1. *The relation*

$$r(n,m) = p(n)\left(\frac{c}{2\sqrt{n}}\right)^{m-1}(m-1)!\ (1 + O(m^2/\sqrt{n}))$$

holds uniformly for $1 \leq m \leq n^{1/4}$.

We hope to be able to improve theorem 1, by giving an asymptotic expansion of $r(n,m)$ for m small, and lower bounds and upper bounds for $r(n,m)$ for m slightly larger than $n^{1/4}$.

Let $n = n_1 + \ldots + n_s$ be a partition of n. Let $k = 1,2,\ldots n$. We say that the partition represents k if k can be written as a subsum $k = n_{i_1} + \ldots + n_{i_t}$ $(1 \leq i_1 < \ldots < i_t \leq s)$. We say that the partition is "practical" if it represents all integers 1, 2, ..., n.

P. Erdős and M. Szalay denoted by M(n) the number of partitions of n which are not practical. In [Erd 1], the number of non practical partitions is proved to be:

$$M(n) = \left\{1 + O\left(\frac{\log^{30} n}{\sqrt{n}}\right)\right\} \frac{\pi}{\sqrt{6n}}\, p(n),$$

which shows that almost all partitions are practical. We shall denote $\tilde{p}(n) = p(n) - M(n)$ the number of practical partitions. We improve the result of P. Erdős and M. Szalay:

THEOREM 2. *Let* $b \in \mathbb{N}$, $b \geq 1$. *There exist real numbers* $\alpha_1, \ldots, \alpha_b$, *such that the following asymptotic expansion is valid, as* $n \to +\infty$:

$$M(n) = \left\{\sum_{a=1}^{b} \alpha_a\, n^{-a/2} + O(n^{-(b+1)/2})\right\} p(n).$$

We have in particular:

$$\alpha_1 = \pi/\sqrt{6};\ \alpha_2 = \pi^2/4 - 1;$$

$$\alpha_3 = \frac{1}{\pi\sqrt{6}} \left(\frac{7}{36}\,\pi^4 - \frac{179}{48}\,\pi^2 + \frac{3}{2} \right);$$

$$\alpha_4 = \frac{1}{\pi^2} \left(\frac{197}{288}\,\pi^6 - \frac{83}{96}\,\pi^4 + \frac{89}{24}\,\pi^2 + \frac{3}{4} \right)$$

We were led to these problems by studying the number of fundamental invariants of binary forms: a lower bound for this number is the number of solutions of a diophantine equation related to those equations which are considered in the theory of partitions (cf. [Dix]).

2. PROOF OF THEOREM 1. First we recall the definition of the mth Bessel polynomial:

$$y_m(x) = 1 + \sum_{k=1}^{m} a_k^{(m)}\, x^k$$

with

$$(8) \qquad a_k^{(m)} = \frac{1}{2^k\, k!} \prod_{j=-k+1}^{k} (m+j) .$$

In particular:

$$a_1^{(m)} = \frac{m(m+1)}{2} \quad \textit{and} \quad a_2^{(m)} = \frac{(m-1)\, m(m+1)(m+2)}{8} .$$

One finds in E. Grosswald's book (cf. [Gro]) many properties of Bessel polynomials. One has

$$y_0(x) = 1$$

$$y_1(x) = 1 + x$$

$$y_2(x) = 1 + 3x + 3x^2$$

$$y_3(x) = 1 + 6x + 15x^2 + 15x^3, \textit{ etc...}$$

They are characterized by several recurrence relations, in particular (cf. [Gro], p. 19):

$$(9) \qquad y_m(x) = (1 + mx)y_{m-1}(x) + x^2 y'_{m-1}(x).$$

With $y_0(x) = 1$, these relations can be used for defining y_m. It is rather easy to get (8) from (9).

LEMMA 1. *Let* $F(x) = (\exp(\sqrt{x}))/\sqrt{x}$; *for the* m^{th} *derivative of* F, *we have:*

$$F^{(m)}(x) = \frac{\exp \sqrt{x}}{2^m x^{(m+1)/2}} y_m(-1/\sqrt{x}).$$

PROOF. The formula is true for $m = 0$. Then one gives a recurrence proof, using (9). We are glad to thank A. Salinier, who observed to us that the polynomials occuring in $F^{(m)}(x)$ were the Bessel's polynomials. (Also cf. [Gro], p. 43. formula (6)).

LEMMA 2. *We have, for* $0 \le x \le \frac{2}{m(m+1)}$:

$$1 - \frac{m(m+1)}{2} x \le y_m(-x) \le 1.$$

PROOF. We have

$$y_m(-x) = \sum_{k=0}^{m} (-1)^k a_k^{(m)} x^k ,$$

with $a_0^{(m)} = 1$. Then, we get:

$$\frac{a_{k+1}^{(m)} x^{k+1}}{a_k^{(m)} x^k} = \frac{x}{2(k+1)} (m+k+1)(m-k) \le x \frac{m(m+1)}{2} \le 1.$$

So $y_m(-x)$ is smaller than its first term 1, and larger than the sum $1 - \frac{m(m+1)}{2} x$ of its two first terms. (Also cf. [Gro], p. 125).

LEMMA 3. *Let* $f:R \to R$, $m \ge 1$, *and* $u_1, u_2, \ldots, u_m \ge 0$. *We define inductively the operator* $D^{(m)}(u_1,\ldots,u_m; f; x)$ *by:*

$$D^{(1)}(u_1; f, x) = f(x) - f(x - u_1)$$

$$D^{(m)}(u_1,\ldots,u_m; f, x) =$$

$$= D^{(m-1)}(u_1,\ldots,u_{m-1};f,x) - D^{(m-1)}(u_1,\ldots,u_{m-1};f,x-u_m).$$

Let $S_m = u_1 + u_2 + \ldots + u_m$.

(*i*) *Assume that the function* f *verifies* $|f(y)| \leq M$ *for* $y \in [x - S_m, x]$; *then*

$$|D^{(m)}(u_1,\ldots,u_m; f,x)| \leq 2^m M.$$

(*ii*) *Assume that the function* f *is* C^m *on* $[x - S_m, x]$; *then there exists* $\xi \in [x - S_m, x]$ *such that:*

$$D^{(m)}(u_1,\ldots,u_m; f,x) = \left(\prod_{i=1}^{m} u_i\right) f^{(m)}(\xi)$$

PROOF: (i) is clear. We prove (ii) by recurrence on m. The assertion is true for m = 1 by the mean value theorem. We assume that the assertion is true for every C^m function and all values of $u_1,\ldots,u_m$. Now we apply the induction hypothesis to the function $\varphi(x) = f(x) - f(x - u_1)$. We get:

$$(10) \qquad D^{m-1}(u_2,\ldots,u_m;\varphi,x) = \left(\prod_{i=2}^{m} u_i\right)\varphi^{(m-1)}(\xi_1) .$$

But the left hand side of (10) is $D^{(m)}(u_1,\ldots,u_m;f,x)$ and

$$\varphi^{(m-1)}(\xi_1) = f^{(m-1)}(\xi_1) - f^{(m-1)}(\xi_1-u_1) = u_1 f^{(m)}(\xi).$$

PROOF OF THEOREM 1. Set $p(0) = r(0,m) = 1$. The generating function of $p(n)$ is $\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} (1 - x^n)^{-1}$. The generating function of $r(n,m)$ is

$$\sum_{n=0}^{\infty} r(n,m)x^n = \prod_{n=m}^{\infty} (1-x^n)^{-1} =$$

$$= \left(\prod_{n=1}^{m-1} (1 - x^n)\right) \left(\sum_{n=0}^{\infty} p(n)x^n\right) .$$

We see that

$$r(n,2) = p(n) - p(n - 1),$$

$$r(n,3) = r(n,2) - r(n-2,2) =$$

$$= p(n) - p(n-1) - p(n-2) + p(n-3)$$

and, in general

$$(11) \qquad r(n,m) = D^{(m-1)} (1,2,\ldots,m-1; p,n).$$

Let $F(x) = (\exp\sqrt{x})/\sqrt{x}$. Then formula (1) can be written:

$$p(n) = \frac{C^3}{2\pi\sqrt{2}} F'(C^2(n - 1/24)) + f_1(n).$$

Then, due to the linearity of the operator $D^{(m)}$, to lemma 3, and to formula (2), there exists $\xi \in \left[n - \frac{m(m-1)}{2}, n\right]$ such that:

$$(12) \qquad r(n,m) = (m-1)!\ \frac{C^{2m+1}}{2\pi\sqrt{2}}\ F^{(m)}(C^2(\xi - 1/24)) +$$

$$+ O(2^{m-1}\ \exp(C\sqrt{n}/2))\ .$$

Let $\zeta = C^2(\xi - 1/24)$. One has:

$$C^2\left(n - \frac{m^2}{2}\right) \le \zeta \le C^2\ n\ ,$$

$$1/(C^2\ n) \le 1/\zeta \le (1/(C^2\ n))(1 + m^2/n)$$

for $m \le \sqrt{n}$; and:

$$(13) \qquad 1/(C\sqrt{n}) \le 1/\sqrt{\zeta} \le (1/C\sqrt{n}))(1 + m^2/(2n)).$$

So we have, for $1 \le m \le n^{1/4}$,

$$\frac{1}{\sqrt{\zeta}} \le \frac{1 + m^2/(2m^4)}{C\ m^2} \le \frac{3}{2\ C\ m^2} \le \frac{1}{m^2} \le \frac{2}{m(m+1)}\ .$$

Using lemma 2, we deduce that:

$$Y_m\left(-\frac{1}{\sqrt{\zeta}}\right) = 1 + O(m^2/\sqrt{n}).$$

Then, we get:

$$\sqrt{\zeta} = C\sqrt{n} + O(m^2/\sqrt{n}),$$

$$\exp(\sqrt{\zeta}) = \exp(C\sqrt{n})\ (1 + O(m^2/\sqrt{n})),$$

$$\zeta^{(m+1)/2} = C^{m+1}\ n^{(m+1)/2}\ \ (1 + O(m^3/n)),$$

and using lemma 1:

$$F^{(m)}(\zeta) = \frac{\exp(C\sqrt{n})}{2^m (C\sqrt{n})^{m+1}} \left(1 + O(m^2/\sqrt{n})\right).$$

Then formulas (12) and (5) complete the proof of theorem 1.

3. PROOF OF THEOREM 2

LEMMA 4. *Let* $n_1, n_2, \ldots, n_j$ *be positive integers, all smaller than* a *with the following property: for all* k, $1 \le k \le a-1$, *there exists a subset* $n_{i_1}, \ldots, n_{i_r}$, $1 \le i_1 < i_2 < \ldots < i_r \le j$, *such that* $n_{i_1} + \ldots + n_{i_r} = k$; *but there is no subset of sum* a. *Then* $n_1 + n_2 + \ldots + \ldots + n_j = a-1$.

PROOF. First we observe that $n_1 + \ldots + n_j \ge a-1$, because $k = a-1$ can be represented as a subsum. So we shall have to prove that $n_1 + \ldots + n_j \ge a$ is impossible.

Let us suppose that $n_1 + \ldots + n_j \ge a$. We take off $n_{i_1}, \ldots, n_{i_r}$ whose sum is a-1. Let us denote by u the smallest remaining n_i; u cannot be equal to one (in that case $n_{i_1} + \ldots + n_{i_r} + u$ would be equal to a). So $u \ge 2$. From our hypothesis, there is a subsum of the n_i's whose sum is u - 1. But from the definition of u, clearly, this subsum must be a subsum of $n_{i_1} + \ldots + n_{i_r}$, let us say $u - 1 = n_{i_1} + \ldots + n_{i_l}$.

Then $\{u, n_{i_{l+1}}, \ldots, n_{i_r}\}$ would be a subset of $\{n_1, \ldots, n_j\}$ whose sum would be a.

LEMMA 5. *With the notations of the introduction, we have:*

$$M(n) = \sum_{1 \le a \le n/2} X(a) \text{ with}$$

$$X(a) = \tilde{p}(a-1)\, r(n-a+1, a+1).$$

PROOF. Let us first notice that lemma 5 allows the computation of M(n) by induction, since $\tilde{p}(a) = p(a) - M(a)$, and r(n,m) is easy to compute. A table of M(n), for $1 \le n \le 100$, is joined at the end of this paper. We are pleased to thank J.P. Massias for carrying out these calculations.

We shall denote by X(a) the number of partitions of n which represent all $k \le a-1$, but which do not represent a. Clearly, if a partition represents k, it does represent also $n-k$ and then, for $a > n/2$, we shall have $X(a) = 0$ and thus we have:

$$M(n) = \sum_{1 \le a \le n/2} X(a).$$

We shall now estimate X(a). Let $n = n_1 + \ldots + n_s$ with $n_1 \le n_2 \le \ldots \le n_s$ be a partition of n which re-

presents all k up to a - 1 but does not represent a. Let us define j by $n_j < a$ and $n_{j+1} > a$. The set $\{n_1, \ldots, n_j\}$ verifies the hypothesis of lemma 4, and thus $\sum_{1 \le i \le j} n_i = a - 1$. Moreover, $(n_1, \ldots, n_j)$ is a practical partition of $a - 1$. Finally $n_{j+1} + \ldots + n_s$ is a partition of $n - a + 1$ all the parts of which are $\ge a + 1$.

LEMMA 6. *For all* $n \ge 0$, $p(n+1) \le 2p(n)$ *holds.*

PROOF. This is obvious for $n = 0$ if we set $p(0) = 1$. Let n be ≥ 1. The number of partitions of $n + 1$ with a part equal to 1 is $p(n)$. Let $n_1 + \ldots + n_s = n + 1$, with $2 \le n_1 \le \ldots \le n_s$. We associate to this partition of $n + 1$ the following partition of n : $n_1 - 1, n_2, \ldots, n_s$.

LEMMA 7. *For* $\alpha \ge 0$ *and for* $m \le \alpha\sqrt{n}$, *we have:*

$$p(n,m) \le \exp((\alpha^3/2 + 2\alpha(1 - \log\alpha))\ \sqrt{n}).$$

PROOF. We shall use the following classical inequalities valid for all n and $1 \le m \le n$ (cf. [Com], p. 126 and [Gup 3], p. 232):

$$(14) \qquad \binom{n-1}{m-1} \le m!\ p(n,m) \le \binom{n + m(m+1)/2 - 1}{m-1}.$$

Observing that $n(n-1)\ldots(n-k+1) \leq \left(n - \frac{k-1}{2}\right)^k$, we deduce from (14):

$$p(n,m) \leq \frac{n^{m-1}}{m!(m-1)!}\left(1 + \frac{m^2}{2n}\right)^{m-1} \leq \frac{n^m}{(m!)^2}\left(1 + \frac{m^2}{2n}\right)^m .$$

By Stirling's formula: $m! \geq m^m e^{-m}\sqrt{2\pi m}$, we obtain:

$$p(n,m) \leq \exp(m^3/2n + m(\log n + 2 - 2 \log m)).$$

But the above right hand side is, for n fixed, increasing in m, for $m \geq 0$, and this completes the proof.

Much more precise estimations for p(n,m) have been given by G. Szekeres: (cf. [Sze 1], [Sze 2], and [Gup 3], ch. 9).

PROOF OF THEOREM 2: From lemma 5, we have:

(15) $$M(n) = S_1 + S_2 + S_3 + S_4$$

with

$$S_1 = \sum_{a=1}^{b} X(a);\ S_2 = \sum_{a=b+1}^{b_0 - 1} X(a);$$

$$S_3 = \sum_{a=b_0}^{b_1} X(a);\ S_4 = \sum_{a=b_1+1}^{\lfloor n/2 \rfloor} X(a),$$

where we set $b_0 = \lfloor n^{1/4} - 1 \rfloor$ and $b_1 = \lfloor 10\sqrt{n} \rfloor$. We shall

first show that each of the sums S_2, S_3 and S_4 is $O(p(n)n^{-(b+1)/2})$. For that we shall replace $X(a)$ by the upper bound $p(a)\ r(n,a+1)$. Then, from theorem 1, there exists an absolute constant γ such that, for $1 \le m \le n^{1/4}$, we have:

$$r(n,m) \le \gamma p(n)(m-1)!\ (C/(2\sqrt{n}))^{m-1}.$$

Finally, from (5) there exists an absolute constant δ, such that, for all $n \ge 1$, we have:

$$p(n) \le \delta \exp(C\sqrt{n}).$$

UPPER BOUND OF S_2. For $b+1 \le a \le b_0 - 1$, we have $X(a) \le f_2(a)$, with

$$f_2(a) = \gamma p(a)\ p(n)\ a!(C/2\sqrt{n})^a\ ,$$

which implies, by lemma 6:

$$\frac{f_2(a+1)}{f_2(a)} = \frac{p(a+1)}{p(a)}\ \frac{C}{2\sqrt{n}}\ (a+1) \le C\ \frac{n^{1/4}}{\sqrt{n}} \le \frac{10}{11}$$

as soon as $n \ge 64$. Thus, for $n \ge 64$, we have:

(16) $$S_2 \le 11\ f_2(b+1) = O(p(n)n^{-(b+1)/2}).$$

UPPER BOUND OF S_3. For $b_0 \le a \le b_1$, we have:

$$X(a) \le p(b_1)\, r(n, b_0+1)$$

$$\le \delta \exp(C\sqrt{10}\, n^{1/4})\, \gamma p(n)\, b_0!\, (C/2\sqrt{n})^{b_0}.$$

But $b_0! \le b_0^{b_0}\, e^{-b_0+1}\, \sqrt{b_0}$, and we obtain:

$$S_3 \le 10\, e\gamma\delta (n)^{5/8} \exp\left[C\sqrt{10}\, n^{1/4} - b_0 \log\left(\frac{2e\sqrt{n}}{Cb_0}\right)\right] p(n).$$

The quantity inside brackets is: $-\frac{1}{4}\, n^{1/4} \log n(1+o(1))$, and thus we have:

$$S_3 = O(p(n)\, n^{-(b+1)/2}). \tag{17}$$

UPPER BOUND OF S_4. For $b_1 + 1 \le a \le n/2$, we use the obvious upper bound:

$$r(n,m) \le p(n, \lfloor n/m \rfloor).$$

Then we have:

$$X(a) \le p(\lfloor n/2 \rfloor)\, r(n, a+1)$$

$$\le \delta \exp(C\sqrt{n/2})\, p(n,m)$$

with $m = \lfloor n/(a+1) \rfloor \le \frac{1}{10}\sqrt{n}$. We use then the upper bound of $p(n,m)$ given by lemma 7, and we get:

$$S_4 \le \delta \frac{n}{2} \exp((C/\sqrt{2}+0.67)\sqrt{n}) \le \frac{\delta n}{2} \exp((C-0.07)\sqrt{n}).$$

By (5), this shows:

$$S_4 = O(p(n)\, n^{-(b+1)/2}). \tag{18}$$

From (15), (16), (17), (18) we conclude:

$$M(n)/p(n) = S_1/p(n) + O(n^{-(b+1)/2}). \tag{19}$$

ESTIMATION OF S_1. We have:

$$S_1 = \sum_{a=1}^{b} \tilde{p}(a-1)\, r(n-a+1, a+1).$$

Lemma 5 allows us to calculate $\tilde{p}$, and we shall use the estimation of $r(n,m)$ given by (11). So, if we define the polynomial:

$$W_b(x) = \sum_{a=1}^{b} \tilde{p}(a-1)\, x^{a-1} (1-x) \ldots (1-x^a)$$

$$= \sum_{\mu=0}^{B} w_\mu^{(b)}\, x^\mu \quad \text{with } B = (b^2+3b-2)/2,$$

we have:

$$S_1 = \sum_{\mu=0}^{B} w_\mu^{(b)}\, p(n-\mu)\ . \tag{20}$$

The first values of W_b are:

$$W_1(x) = 1 - x$$
$$W_2(x) = 1 - x^2 - x^3 + x^4$$
$$W_3(x) = 1 - 2x^3 + x^6 + x^7 - x^8$$
$$W_4(x) = 1 - 2x^4 - 2x^5 + x^6 + x^7 + 3x^8 - 2x^{11} - 2x^{12} + 2x^{13}.$$

Using the same argument as for (4), we get:

$$p(n-\mu) = \frac{\exp(C\sqrt{n})}{4\pi\sqrt{2}\,n}\, g(\mu + 1/24,\ 1/\sqrt{n}) + f_1(n-\mu). \tag{21}$$

Let $T_b(\lambda, t)$ be the Taylor polynomial of $g(\lambda, t)$ with respect to t, of degree b, near $t = 0$. For instance, we have,

$$T_3(\lambda,t) = C - \left(1+\frac{C^2\lambda}{2}\right)t + \left(\frac{3C\lambda}{2} + \frac{C^3\lambda^2}{8}\right)t^2 - \tag{22}$$

$$- \left(\frac{3\lambda}{2} + \frac{3C^2\lambda^2}{4} + \frac{C^4\lambda^3}{48}\right) t^3 .$$

For μ fixed, we deduce from (21) and (2) the following asymptotic expansion, for $n \to +\infty$

$$p(n-\mu) = \frac{\exp(C\sqrt{n})}{4\pi\sqrt{2}\,n}\, (T_b(\mu + 1/24,\ 1/\sqrt{n}) + \tag{23}$$

$$+ O(n^{-(b+1)/2})),$$

and thus, from (20) we have:

$$S_1 = \frac{\exp(C\sqrt{n})}{4\pi\sqrt{2}\,n} \left[\sum_{\mu=0}^{B} w_\mu^{(b)}\, T_b(\mu+1/24, 1/\sqrt{n}) + O(n^{-(b+1)/2})\right]. \tag{24}$$

Dividing by p(n) and using (21) with $\mu = 0$, we get:

$$S_1/p(n) = \frac{\sum_{\mu=0}^{B} w_\mu^{(b)}\, T_b(\mu+1/24,\ 1/\sqrt{n})}{T_b(1/24,\ 1/\sqrt{n})} + O(n^{-(b+1)/2}).$$

We now calculate the Taylor expansion of the above quotient with an error term $O(n^{-(b+1)/2})$, and with (19) this ends the proof of theorem 2.

CALCULATION OF THE COEFFICIENTS α_i. We shall now suppose $b = 3$ and $B = 8$. We set:

$$\sigma_i = \sum_{\mu=0}^{B} w_\mu^{(b)} \mu^i ; \quad \tau_i = \sum_{\mu=0}^{B} w_\mu^{(b)} (\mu + 1/24)^i .$$

One has

$$\sigma_0 = 0; \ \sigma_1 = -1; \ \sigma_2 = 3; \ \sigma_3 = -7$$

$$\tau_0 = 0; \ \tau_1 = \frac{1}{24}\sigma_0 + \sigma_1 = -1;$$

$$\tau_2 = 35/12; \ \tau_3 = -1273/192.$$

From (22) and (24), we have:

$$(25) \qquad S_1 = \frac{\exp C\sqrt{n}}{4\pi\sqrt{2}\, n} \left[\tau_0 C - (\tau_0 + \frac{C^2}{2}\tau_0)\frac{1}{\sqrt{n}} + \left(\frac{3C\tau_1}{2} + \frac{C^3\tau_2}{8} \right) \frac{1}{n} - \right.$$

$$\left. - \left(\frac{3}{2}\tau_1 + \frac{3C^2}{4}\tau_2 + \frac{C^4}{48}\tau_3 \right) \frac{1}{n^{3/2}} + O(n^{-2}) \right] =$$

$$= \frac{\exp C\sqrt{n}}{4\pi\sqrt{2}\, n} \left[\frac{C^2}{2}\frac{1}{\sqrt{n}} + \left(\frac{3C}{2} + \frac{35}{96}C^3 \right) \frac{1}{n} + \right.$$

$$\left. + \left(\frac{3}{2} - \frac{35}{16}C^2 + \frac{1273}{9216}C^4 \right) \frac{1}{n^{3/2}} + O(n^{-2}) \right] .$$

From (22), with $\lambda = 1/24$, we deduce:

$$(26) \qquad T_3(1/24,t))^{-1} = \frac{1}{C}\left[1 + \left(\frac{1}{C} + \frac{C}{48}\right)t + \right.$$

$$\left. + \left(\frac{1}{C^2} - \frac{1}{48} + \frac{C^2}{4608}\right)t^2 + O(t^3)\right],$$

and, multiplying (25) by (26) with $t = 1/\sqrt{n}$, we obtain:

$$S_1/p(n) = \frac{C}{2\sqrt{n}} + \left(-1 + \frac{3}{8}C^2\right)\frac{1}{n} +$$

$$+ \left(\frac{1}{2C} - \frac{179}{96}C + \frac{7}{48}C^3\right)\frac{1}{n^{3/2}} + O(n^{-2}).$$

Replacing C by its value $\pi\sqrt{2/3}$, we get the announced values α_1, α_2, α_3. The above calculation has been checked by the computer algebra systems MACSYMA and MAPLE. We are pleased to thank J.P. Massias and F. Morain for computing the α_i's for $1 \le i \le 20$. It can be seen that α_i is a polynomial in π divided by a power of π. We give below an approximate value of α_i.

i	1	2	3	4	5	6	7	8
α_i	1.28	1.47	-2.13	61.9	-600.0	$9.88\ 10^3$	$-1.25\ 10^5$	$1.83\ 10^6$

i	9	10	11	12	13	14
α_i	$-2.94\ 10^7$	$6.09\ 10^8$	$-1.46\ 10^{10}$	$3.91\ 10^{11}$	$-1.11\ 10^{13}$	$3.26\ 10^{14}$

i	15	16	17	18	19	20
α_i	$-9.54\ 10^{15}$	$2.83\ 10^{17}$	$-8.90\ 10^{18}$	$3.12\ 10^{20}$	$-1.23\ 10^{22}$	$5.20\ 10^{23}$

TABLE OF $M(n)$ AND $\tilde{p}(n)$ FOR $n \leq 100$

n	p(n)	M(n)	$\tilde{p}(n)$	n	p(n)	M(n)	$\tilde{p}(n)$
1	1	0	1	51	239943	57695	182248
2	2	1	1	52	281589	67628	213961
3	3	1	2	53	329931	77300	252631
4	5	3	2	54	386155	90242	295913
5	7	3	4	55	451276	103131	348145
6	11	6	5	56	526823	119997	406826
7	15	7	8	57	614154	136866	477288
8	22	12	10	58	715220	158990	556230
9	30	14	16	59	831820	180968	650852
10	42	22	20	60	966467	209586	756881
11	56	25	31	61	1121505	238533	882972
12	77	38	39	62	1300156	275425	1024731
13	101	46	55	63	1505499	312897	1192602
14	135	64	71	64	1741630	360806	1380824
15	176	76	100	65	2012558	409237	1603321
16	231	106	125	66	2323520	470659	1852861
17	297	124	173	67	2679689	533593	2146096
18	385	167	218	68	3087735	612257	2475478
19	490	199	291	69	3554345	693097	2861248
20	627	261	366	70	4087968	794162	3293806
21	792	309	483	71	4697205	897718	3799487
22	1002	402	600	72	5392783	1026447	4366336
23	1255	471	784	73	6185689	1159767	5025922
24	1575	604	971	74	7089500	1323290	5766210
25	1958	714	1244	75	8118264	1493120	6625144
26	2436	898	1538	76	9289091	1701634	7587457
27	3010	1053	1957	77	10619863	1917673	8702190
28	3718	1323	2395	78	12132164	2181368	9950796
29	4565	1542	3023	79	13848650	2456810	11391840
30	5604	1911	3693	80	15796476	2789799	13006677
31	6842	2237	4605	81	18004327	3138471	14865856
32	8349	2745	5604	82	20506255	3559678	16946577
33	10143	3201	6942	83	23338469	4000029	19338440
34	12310	3913	8397	84	26543660	4529625	22014035
35	14883	4536	10347	85	30167357	5086932	25080425
36	17977	5506	12471	86	34262962	5751522	28511440
37	21637	6402	15235	87	38887673	6452197	32435476
38	26015	7706	18309	88	44108109	7287542	36820567
39	31185	8918	22267	89	49995925	8167149	41828776
40	37338	10719	26619	90	56634173	9211235	47422938

TABLE OF M(n) AND $\tilde{p}(n)$ FOR $n \leq 100$

n	p(n)	M(n)	$\tilde{p}(n)$	n	p(n)	M(n)	$\tilde{p}(n)$
41	44583	12364	32219	91	64112359	10316448	53795911
42	53174	14760	38414	92	72533807	11619747	60914060
43	63261	17045	46216	93	83010177	13001601	69008576
44	75175	20234	54941	94	92669720	14629286	78040434
45	89134	23296	65838	95	104651419	16353590	88297829
46	105558	27600	77958	96	118114304	18378039	99736265
47	124754	31678	93076	97	133230930	20531393	112699537
48	147273	37365	109908	98	150198136	23044982	127153154
49	173525	42910	130615	99	169229875	25722031	143507844
50	204226	50371	153855	100	190569292	28844400	161724892

REFERENCES

[Com] COMTET, L., Analyse combinatoire, tome 1, Presses Universitaires de France, Paris, 1970.

[Dix] DIXMIER, J., ERDŐS, P. and NICOLAS, J.L., Sur le nombre d'invariants fondamentaux des formes binaires, CRAS, Paris, t. 305, série I, 1987, p. 309-322.

[Erd 1] ERDŐS, P. and SZALAY, M., On some problems of J. Dénes and P. Turan, Studies in pure Mathematics to the memory of P. Turan, Editor P. Erdős, Budapest 1983, p. 187-212.

[Erd 2] ERDŐS, P. and SZALAY, M., On the statistical theory of partitions, Coll. Math. Soc. János Bolyai, 34, Topics in classical number theory, Budapest 1981, p. 397-450.

[Erd 3] ERDŐS, P., NICOLAS, J.L. and SZALAY, M., Partitions into parts which are unequal and large, to be published in the proceedings of "Journées Arithmétiques", Ulm, 1987.

[Gro] GROSSWALD, E., Bessel Polynomials, Lecture notes in mathematics n° 698, Springer Verlag, 1978.

[Gup 1] GUPTA, H., GWYTHER, C.E. and MILLER, J.C.P., Table of partitions, Cambridge University Press, 1962.

[Gup 2] GUPTA, H., A formula in partitions, J. Indian Math. Soc. (N.S.) t. 6, 1942, p. 115-117.

[Gup 3] GUPTA, H., Selected topics in number theory, Abacus Press, 1980.

[Gup 4] GUPTA, H., Tables of partitions, Indian Math. Soc., Madras, 1939.

[Her] HERZOG, J., Gleichmässige asymptotische Formeln für parameterabhängige Partitionen-funktionen, Thesis of the University J.W. Goethe, Frankfurt am Main, March 1987.

[NIC] NICOLAS, J.L., Sur les entiers n pour lesquels il y a beaucoup de groupes abéliens d'ordre n, Ann. Inst. Fourier, t. 28, n° 4, 1978, p. 1-16.

[Odl] ODLYZKO, A.M., Differences of the partition function, to appear in Acta Arithmetica 1988, dedicated to P. Erdős.

[Rad] RADEMACHER, H., Topics in analytic number theory, Die Grundlehren der mathematischen Wissenschaften, Band 169, Springer Verlag, 1973.

[Ram] HARDY, G.H. and RAMANUJAN, Asymptotic formulae in combinatory analysis, Proc. of the London Math. Soc. 2, t. 17, 1918, p. 75-115 and Collected Papers of S. Ramanujan, §36, p. 276-309.

[Sze] SZEKERES, G., An asymptotic formula in the theory of partitions, Quart. J. Math. Oxford, (2), t. 2, 1951, p. 85-108.

[Sze] SZEKERES, G., Some asymptotic formulae in the theory of partitions II , Quart. Oxford, (2), t. 4, 1953, p. 96-111.

DIXMIER, J.
IHES
35, route de Chartres
F-91440 Bures-sur-Yvette

NICOLAS, J.L.
Département de Mathématiques
Université de Limoges
123 avenue Albert Thomas
F-87060 Limoges Cédex

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

APPLICATIONS OF ELEMENTARY FUNCTIONAL ANALYSIS TO THE STUDY OF ARITHMETIC FUNCTIONS

ELLIOTT P.D.T.A.

Consider the complex valued additive function $f(n) = \Sigma f(q)$, $q \| n$, restricted to the interval $1 \le n \le x$. We regard the $f(q)$ as determining a vector in the space C^s with s the number of prime-powers q not exceeding x. For $\alpha \ge 1$ we may topologize C^s with the norm

$$\|f\|_\alpha = \left(\sum_{q \le x} \frac{|f(q)|^\alpha}{q} \left(1 - \frac{1}{q_o}\right) \right)^{1/\alpha},$$

where q_o denotes the prime of which q is a power. We can also think of C^s as the space of functions on s points, with a measure du that assigns weight $q^{-1}(1 - q_o^{-1})$ to the q-coordinate point. In an obvious abuse of notation I write L^α for this Banach space.

Similarly, $\mathbb{M}^\beta$ will denote the space $C^{[x]}$ of $[x]$-tuples a, one coordinate for each positive integer not exceeding x, topologized with

$$\|a\|_\beta = \left(\frac{1}{[x]} \sum_{n \le x} |a_n|^\beta\right)^{1/\beta} .$$

Here the associated frequency measure assigns weight $[x]^{-1}$ to the nth point. Note that this measure assigns weight 1 to the whole space $C^{[x]}$, whereas the earlier measure du assigns to C^S the unbounded weight loglog x + O(1).

The classical Turán-Kubilius inequality asserts that the operator $A_2 : L^2 \to \mathbb{M}^2$ given by $(A_2 f)(n) = f(n) - \mu$, with

$$\mu = \int f du = \sum_{q \le x} \frac{f(q)}{q} \left(1 - \frac{1}{q_o}\right) ,$$

has norm bounded uniformly in $x \ge 2$. More generally, the same operator, but denoted by A_α has uniformly bounded norm when viewed as between $L^2 \cap L^\alpha$ and $\mathbb{M}^\alpha$ for $\alpha \ge 2$, and $(L^2 \cap L^{\alpha'})'$ and $\mathbb{M}^\alpha$ for $1 < \alpha \le 2$. Here $L^\alpha \cap L^\delta$ denotes the space C^S with norm $\max(\| \|_\alpha ; \| \|_\delta)$ and $'$ denotes either the dual of a space, or a number given by $\alpha^{-1} + (\alpha')^{-1} = 1$, as the case may be.

The map $I - A_2^* A_2$ of the Hilbert space L^2 into itself is self-adjoint, and its spectrum can be largely obtained. It has (simple) eigenvalues $(-1)^{j+1}/j + + O((\log n)^{-1/2})$, $j = 1,2,\ldots$. Here $*$ denotes the adjoint of A.

In the more general situation we replace $A_2^* A_2$ by A'_α, A_α using an appropriate dual of A_α, and identifying the space $M^{\alpha'}$ with $(M^\alpha)'$. Of course the spectrum of $I - A'_\alpha, A_\alpha$ is unchanged, but the operator acts on $L^2 \cap L^\alpha$ or $(L^2 \cap L^{\alpha'})'$ into itself, and it requires considerable further argument to show that eigenvectors d_j, first chosen to have norm 1 in the space L^2, also have norms that are bounded uniformly with respect to x in each of these new intersection spaces.

A description of the derivation of this theory I gave in Oberwolfach, Germany, last October (see also, Elliott [4]). A detailed and historical account of its background, and of various applications to number theory, may be found in my survey paper [1]. Here I consider shift operators and their rôle in the study of the differences of additive functions. It will be convenient to define $f(0) = 0$.

THEOREM. *For each* $\alpha > 1$ *there is a constant* c *so that*

$$x^{-1}|F| + \|f - F\log\| \ll \sup_{x\le y\le x^c}\left\{y^{-1}\sum_{x<n\le y}|f(n)-f(n-1)|^\alpha\right\}^{1/\alpha}.$$

For $\alpha \ge 2$ *the norm is that on* $L^2 \cap L^\alpha$, *for* $1 < \alpha < 2$ *it is that on* $(L^2 \cap L^{\alpha'})'$. *The function* F *is* $(f, \log)\|\log\|_2^{-2}$ *in terms of the inner-product on* L^2. *The implied constant depends only upon* α.

We define a shift operator E on M^β to itself by $a_n \to a_{n+1}$ if $n + 1 \le x$, $a_{[x]} \to 0$. For $r \ge 2$, $E^r = E(E^{r-1})$. Similarly E^{-1} takes a_n to a_{n-1}, and a_1 to 0, whilst $E^{-r} = E^{-1}(E^{-(r-1)})$. Direct calculation shows that $(E^r)' = E^{-r}$. The general line of argument in the proof of the theorem is to begin with

$$\|A'_\alpha,(I - E^{-1})A_\alpha f\| \ll \|(I - E^{-1})A_\alpha f\|,$$

since A'_α, is uniformly bounded. Here the dominating norm is

$$\left\{\frac{1}{[x]}\sum_{2\le n\le x}|f(n) - f(n-1)|^\alpha + \frac{1}{[x]}|\mu|^\alpha\right\}^{1/\alpha}$$

which is largely of the form needed in the theorem. As

before A'_α, A_α is manageable, but the new operator $A'_\alpha, E^{-1}A_\alpha$ appears. If we could ignore it, then we would obtain results for differences which would be of the same quality as those for a single additive function. As an illustration, with the case $\alpha = 2$, $\|A_2E^{-1}A_2\|^2$ lies between absolute constant multiples of

$$x^{-2} \sum_{q\le x} q \left| \sum_{\substack{n\le x-1 \\ n\equiv 1 (\mathrm{mod}\ q) \\ n\not\equiv 1 (\mathrm{mod}\ q\, q_0)}} f(n) - \frac{1}{q}\left(1 - \frac{1}{q_0}\right) \sum_{n\le x-1} f(n) \right|^2 .$$

One recognizes an expression of the type occurring in the study of the Large Sieve. Instead of many residue classes, attention is confined to essentially only one class (better than usual!); but the moduli q run all the way up to x (worse than usual!).

From the uniform boundedness of the operators A_α we see that this expression is $\ll \|f\|^2 \le \sum q^{-1}|f(q)|^2$, $q \le x$. This is already interesting, but for our approach to succeed we need more, something which is essentially smaller than $\|f\|^2$ in the upper bound. At present I am only able to establish a partial result. For $0 < \delta \le 1$ let P_δ denote the projection of C^S into itself given by $f(q) \to 0$ if $q > x^\delta$, but $f(q)$ to remain the same for $q \le x^\delta$. This projection preserves the fraction δ of the measure du, so-to-speak. Then I can prove (essentially):

LEMMA: *For each* $\alpha > 1$ *there are positive* δ, γ *so that*

$$\| P_\delta A'_\alpha, E^r A_\alpha \| \ll (\log x)^{-\gamma}$$

provided $r \neq 0$ *and* x *is sufficiently large. The values of* δ, γ *do not depend upon* r.

We have bought the improvement $(\log x)^{-\gamma}$ at the price of cutting down the size of the moduli q to $q \leq x^\delta$. Note, however, that there is no restriction upon the function f beyond that it be additive. This is very important. The validity of a result of the type given in this lemma, without side conditions upon the $f(q)$, is not at all apparent, and I was driven to it by stages (refs. [2], [3], [4], [5]). Unlike with the Bombieri-Vinogradov theorem, we cannot take γ arbitrarily large. For $\alpha = 2$, $\delta < 1/2$ we may take any fixed $\gamma < 1/2$, and this is in the nature of things. Counter-examples show that no matter what the size of δ, with $\gamma > 1/2$ the result is false.

The proof of the lemma involves the introduction of larger spaces, and the consideration of fractional-power Large-Sieves. In particular I employ the independence of random variables m at a time, where m goes up as the α in L^α goes down. In particular, this generalizes a

view of Rényi, who applied the idea of approximately uncorrelated random variables when $\alpha = 2$. Duality is applied many times.

The presence of the projection P_δ is responsible for the appearance of the constant c in the theorem. The proof of the theorem involves approximate functional equations because we cannot employ a spectral decomposition theorem to study $P_\delta A'_\alpha, A_\alpha$; and iterations to overcome the fact that $\delta < 1$.

CONJECTURE. *To each space* $(L^2 \cap L^{\alpha'})'$ *if* $1 < \alpha \leq 2$; $L^2 \cap L^\alpha$ *if* $\alpha \geq 2$, *there is a positive constant* γ, *so that for each non-zero* r

$$\| A'_\alpha, E^r A_\alpha \| << (\log x)^{-\gamma} .$$

A likely value for γ is $1/\alpha'$. Note that the dual of $A'_\alpha, E^r A_\alpha$ has the same form, but with $-r$ in place of r. Thus we need only consider one of the ranges $1 < \alpha \leq 2$; $2 \leq \alpha < \infty$. It also enables us to deduce from the lemma that

$$\| A'_\alpha, E^r A_\alpha P_\delta \| << (\log x)^{-\gamma} .$$

For example, the following inequality is valid for each fixed $r \neq 0$, $\delta < 1/180$.

$$\sum_{q\le x} q^2 \Big| \sum_{\substack{n\le x \\ n\equiv r(\mathrm{mod}\ q) \\ n\not\equiv r(\mathrm{mod}\ q\, q_0)}} f_\delta(n) - \frac{1}{q} \sum_{\substack{n\le x \\ (n,q)=1}} f_\delta(n) \Big|^3 \ll$$

$$\ll \frac{x^3}{(\log x)^{1/4}} (\log\log x)^5 \sum_{\ell\le x} \frac{|f(\ell)|^3}{\ell}$$

where ℓ, q denote prime-powers, and $f_\delta(n)$ denotes the truncated additive function $\Sigma f(\ell)$, $\ell \| n$, $\ell \le x^\delta$. The conjecture asserts that with possibly a different constant in place of the 1/4, this truncation can be removed.

REFERENCES

[1] ELLIOTT, P.D.T.A., Functional analysis and additive arithmetic functions. *Bull. American Math. Soc.* 16 (2) (1987), 179-223.

[2] ELLIOTT, P.D.T.A., On the difference of additive functions. *Mathematika* 24 (1977), 153-165.

[3] ELLIOTT, P.D.T.A., On additive arithmetic functions f(n) for which f(an + b) - f(cn + d) is bounded. *Journ. Number Theory* 16 1983 , 285-310.

[4] ELLIOTT, P.D.T.A., *Arithmetic Functions and Integer Products*. Grund. der math. Wiss. 272, Springer-Verlag, New York, Berlin, Tokyo, 1985.

[5] ELLIOTT, P.D.T.A., Additive arithmetic functions on arithmetic progressions. *Proc. London Math. Soc.* (3) 54 (1987), 15-37.

ELLIOTT P.D.T.A.
Boulder, Colorado 80309

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE DISTRIBUTION OF VALUES OF A CERTAIN CLASS OF ARITHMETIC FUNCTIONS AT CONSECUTIVE INTEGERS

PAUL ERDŐS and ALEKSANDAR IVIĆ

1. INTRODUCTION

The purpose of this paper is to study several aspects of the problem of the distribution of values of certain arithmetic functions, especially of the values at consecutive integers. Our main motivation is the function $a(n)$, which represents the number of non-isomorphic Abelian groups with n elements. This is a well-known multiplicative function which satisfies $a(p^{\alpha}) = P(\alpha)$, where henceforth p will denote primes and $P(k)$ will denote the number of (unrestricted) partitions of k. It is known that $a(n)$ possesses a positive mean value, and more precisely one has

$$(1.1) \qquad \sum_{n\le x} a(n) = \sum_{m=1}^{3} A_m x^{1/m} + R(x), \quad A_m = \prod_{k=1,k\neq m}^{\infty} \zeta(k/m).$$

It was proved long ago by P. Erdős and G. Szekeres [3] that $R(x) \ll x^{1/2}$, and after many subsequent improvements the best known bound is $R(x) \ll x^{97/381}\log^{35}x$, which is due to G. Kolesnik [17]. There are several interesting arithmetic aspects of the function $a(n)$ and similar functions. For example, $a(p) = 1$ for every prime p, so that $a(n) = a(s(n))$, where $s(n)$ is the squarefull part of n. Namely every integer $n \geq 1$ may be uniquely decomposed as $n = q(n)s(n)$, $(q(n),s(n) = 1)$, where $q(n)$ is squarefree and $s(n)$ is squarefull (s is squarefull if $p^2 | s$ whenever $p | s$). Nonnegative, integer-valued arithmetic functions $f(n)$ such that $f(n) = f(s(n))$ for every $n \geq 1$ were called functions with squarefull kernel, or simply s-functions by A. Ivić and G. Tenenbaum [16]. It is to be noted that s-functions are not necessarily multiplicative: $\Omega(n) - \omega(n)$ is clearly an additive s-function, where as usual $\Omega(n)$ and $\omega(n)$ denote the number of all prime factors of n and the number of distinct prime factors of n, respectively. It was shown in [16] by a simple argument that the local density

$$(1.2) \qquad d_k = \lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x, f(n)=k} 1$$

of an s-function always exists for any fixed $k \geq 0$. In fact, it was proved in [16] that an asymptotic formula implying (1.2) with the uniform error term $O(x^{1/2}\log^2 x)$

exists. More precise results on local densities of $a(n)$ and related functions were proved by E. Krätzel [20] and A. Ivić [15]. The property that $a(n)$ is an s-function is essential in the proof of the asymptotic formulas

$$(1.3) \qquad \sum_{n\le x,\, a(n)=a(n+1)} 1 = Ax + O(x^{3/4}\log^4 x),$$

$$\sum_{n\le x} a(n)(\Omega(n+1) - \omega(n+1)) = Bx + O(x^{3/4+\varepsilon}),$$

where $A, B > 0$ are two constants which may be explicitly evaluated. These formulas are new, and in proving them we shall also make use of the order result

$$(1.4) \qquad a(n) \le \exp\left(\left(\frac{\log 5}{4} + \varepsilon\right)\frac{\log n}{\log\log n}\right) \quad (n \le n_0(\varepsilon)).$$

This was proved by E. Krätzel [19], and later sharpened by W. Schwarz and E. Wirsing [28], and J.-L. Nicolas [26]. The above mentioned properties of $a(n)$ are essentially the only ones needed in the proof of (1.3). In 2. we shall prove a more general result than (1.3) for suitable s-functions satisfying a mild growth condition analogous to (1.4). In order to avoid unnecessary technicalities we have not tried to obtain the most general possible form of our results. This is also true of other sections, where the results obtained for $a(n)$ may be readily generalized to many other multiplicative functions.

It will turn out, however, that the method used in proving Theorem 1 and Theorem 2 in 2. (the appropriate generalizations of (1.3)) may yield asymptotic formulas for other related arithmetic sums. This is discussed in 3. where several other applications of our method are discussed. These include the asymptotic formulas

$$(1.5) \qquad \sum_{n\le x} a(n)d(n+1) = C_1 x \log x + C_2 x + O(x^{8/9+\varepsilon})$$

and

$$(1.6) \qquad \sum_{n\le x} a(n)\omega(n+1) = D_1 x \log\log x + D_2 x + O(x/\log x)$$

with $C_1, D_1 > 0$, which seems to be new.

In [15] A. Ivić defined the functions $C(x)$, $D(x)$, $E(x)$ as follows: $C(x)$ denotes the number of distinct values taken by $a(n)$ for $n \le x$, $D(x)$ denotes the number of $n \le x$ such that $n = a(m)$ for some integer m, $E(x) = \sum_{n\le x} b(n)$, where $b(n)$ is the number of solutions in squarefull s of the equation $n = a(s)$ for a fixed n. The functions $C(x)$ and $D(x)$ determine to a great extent the distribution of values of $a(n)$, and it is obvious that

$$(1.7) \qquad C(x) \le D\left(\exp\left\{\left(\frac{\log 5}{4} + \varepsilon\right)\frac{\log x}{\log\log x}\right\}\right), \quad D(x) \le E(x).$$

It was proved in [15] that

$$(1.8) \qquad C(x) \le \exp((3^{-1/2}\, 2\pi + \varepsilon)(\log x/\log\log x)^{1/2}) \quad (x \ge x_0(\varepsilon)),$$

and the significance of $E(x)$ is that it may be fairly precisely evaluated. Thus it was shown in [15] that, as $x \to \infty$,

$$(1.9) \qquad E(x) = \exp((B+o(1))\log^{2/3} x), \quad B = \frac{3}{2}(6\zeta(3)\pi^{-2})^{1/3},$$

and this formula was refined by J. Herzog and W. Schwarz [12], [13]. Problems involving the estimation of $C(x)$ and $D(x)$ are discussed in 4. where explicit dependence of these functions on the structure of prime factors of the partition function $P(k)$ is exhibited. It is very plausible to conjecture that

$$(1.10) \qquad C(x) = \exp(\log^{1/2+o(1)} x), \quad D(x) = \exp(\log^{2/3+o(1)} x),$$

$$(x \to \infty)$$

and these formulas are proved if a certain conjecture involving the function $P(k)$ is assumed. Our construction of the lower bound for $C(x)$ may be generalized to various other multiplicative functions besides $a(n)$. Thus if $d_k(n)$ represents the number of ways n may be written as a product of $k \geq 2$ fixed factors ($d_2(n) = d(n)$) and $C(x)$ is again the corresponding number of distinct values of $d_k(n)$ for $n \leq x$, then our construction gives

$$(1.11) \qquad \exp(E_1(k)(\log x)^{1/2}/\log\log x) \ll C(x) \ll$$

$$\ll \exp(E_2(\log x/\log\log x)^{1/2})$$

for some $E_1(k)$, $E_2 > 0$. This seems to be new for $k > 2$, but for $k = 2$ (i.e. for $d(n)$) this problem has been practically solved by P. Erdős and L. Mirsky [5], who proved

$$(1.12) \qquad C(x) = \exp((2\pi(2/3)^{1/2} + o(1))(\log x)^{1/2}/\log\log x) \quad (x \to \infty).$$

For some recent results concerning (1.12) and the related B-numbers defined in [5], see the works of M. Nair and P. Shiu [25], [29].

The aforementioned paper of Erdős and Mirsky considered problems concerned with long blocks of consecutive integers such that the values of $d(n)$ at these integers are all distinct. It was shown that there exist infinitely many n such that $d(n+1)$, $d(n+2)$, ..., ..., $d(n+k)$ are all distinct, where $k = [c(\log n)^{1/2}/\log\log n]$. It was also conjectured that $d(n) = d(n+1)$ has infinitely many solutions, and this difficult problem has been only recently solved in the affirmative by D.R. Heath-Brown [11]. Both of these problems for $a(n)$ are duscussed in 5. and naturally they can be considered for various other arithmetic functions. The intrinsic property that $a(p) = 1$ gives easily the existence of infinitely many n such that $a(n) = a(n+1) = a(n+2)$ holds. This follows from the old result of L. Mirsky [23] that

$$(1.13) \qquad \sum_{n \le x} \mu^2(n)\mu^2(n+1)\mu^2(n+2) = \prod_p (1 - 3p^{-2})x + O(x^{2/3+\varepsilon}),$$

ORSZ. SZECHÉNYI KÖNYVTÁR

since $a(n) = a(n+1) = a(n+2) = 1$ if $\mu^2(n)\mu^2(n+1)\mu^2(n+2) = 1$. Hence this problem for $a(n)$ is considerably easier than the corresponding problem for $d(n)$ (not much seems to be known about n for which $d(n) = d(n+1) = d(n+2)$). We shall prove that there are infinitely many n such that the values $a(n+1), \ldots, a(n+t)$ are all distinct for $t = [C(\log n/\log\log n)^{1/2}]$ $(C > 0)$, and infinitely many n such that $a(n+1) = \ldots = a(n+k)$ for $k = [D \log n \log\log\log n/(\log\log n)^2]$ $(D > 0)$. Quantitative forms of these results are contained in Theorem 6 and 7 of 5.

Finally we wish to thank A. Schinzel for kindly letting us use his unpublished result (Lemma 2) on prime factors of the partition function.

2. ASYMPTOTIC FORMULAS FOR CERTAIN SUMMATORY FUNCTIONS

In this section we shall prove a general result which contains (1.3). First we make the following

DEFINITION. Let B denote the class of nonnegative, integer-valued s-functions $b(n)$ (i.e. $b(n) = b(s(n))$ for $n \geq 1$) such that $b(n) \ll n^{\varepsilon}$ for any $\varepsilon > 0$.

In view of (1.4) it follows that $a(n)$ (generated by $\zeta(s)\zeta(2s)\zeta(3s)\ldots$) belongs to B, and many other multiplicative functions also belong to B. Two further

examples are $S(n)$ (the number of non-isomorphic semi-simple rings with n elements, generated by $\prod_{m,r>1} \zeta(mr^2s)$) and $d^{(e)}(n)$ (the number of exponential divisors of n, defined by the relation $d^{(e)}(p^\alpha) = d(\alpha)$). But as noted in 1. s-functions need not be multiplicative, and e.g. $\Omega(n) - \omega(n)$ belongs to B, since $\Omega(n) - \omega(n) \le \frac{\log n}{\log 2} - 1$ for $n \ge 1$), and other examples of additive functions from B may be readily found.

Our aim in this section is to study the asymptotic behaviour of the sums $\sum_{n\le x, f(n)=g(n+1)} 1$ and $\sum_{n\le x} f(n)g(n+1)$ when $f,g \in B$. The growth condition imposed on the functions of B is a mild one, and a condition of this sort is necessary if one wishes to avoid trivial results. One expects that both of the above sums are asymptotic to Cx for some $C \ge 0$. This, and much more, turns out to be true. Our results are contained in the following two theorems.

THEOREM 1. Let $f(n)$ and $g(n)$ be two functions belonging to B. If s_1, s_2 denote squarefull numbers, then we have

$$(2.1) \qquad \sum_{n\le x, f(n)=g(n+1)} 1 = Ax + O(x^{3/4}\log^4 x),$$

where

$$(2.2) \qquad A = A(f,g) = \frac{6}{\pi^2} \sum^{\infty}_{s_1,s_2=1,(s_1,s_2)=1,f(s_1)=g(s_2)} \frac{1}{s_1 s_2} \times$$

$$\times \prod_{p \mid s_1 s_2} \left(1 - \frac{1}{p}\right) \prod_{p \nmid s_1 s_2} \left(1 - \frac{2}{p^2}\right).$$

THEOREM 2. Let $f(n)$ and $g(n)$ be two functions belonging to B. If s_1, s_2 denote squarefull numbers, then we have

$$\sum_{n \le x} f(n) g(n+1) = Cx + O(x^{3/4+\varepsilon}), \tag{2.3}$$

where

$$C = C(f,g) = \frac{6}{\pi^2} \sum_{s_1, s_2 = 1, (s_1, s_2) = 1}^{\infty} \frac{f(s_1) g(s_2)}{s_1 s_2} \times \prod_{p \mid s_1 s_2} \left(1 - \frac{1}{p}\right) \prod_{p \nmid s_1 s_2} \left(1 - \frac{2}{p^2}\right). \tag{2.4}$$

Note that $A > 0$ if $f(s_1) = g(s_2)$ has at least one solution in squarefull s_1, s_2 such that $(s_1, s_2) = 1$, while $C > 0$ if $f(s_1), g(s_2) > 0$ for at least one pair s_1, s_2 such that $(s_1, s_2) = 1$. It may be remarked that Theorem 1 and Theorem 2 have relatively wide applicability, since $f(n)$, $g(n) \in$ B implies both $f(n)g(n) \in$ B and $f^k(n) \in$ B for any integer $k \ge 1$. The proofs of both theorems depend on a certain asymptotic formula involving squarefree numbers. This is

LEMMA 1. Let a,b be two given natural numbers such that (a,b) = 1 and let

$$(2.5)\qquad S = \sum_{ka-lb=1,\, lb\le x,\, (k,a)=(l,b)=1} \mu^2(k)\mu^2(l),$$

where k,l denote natural numbers. Then uniformly for $1 \le b \le x^{\frac{1}{2}}$

$$(2.6)\qquad S = \frac{6x}{\pi^2 ab} \prod_{p\mid ab}\left(1-\frac{1}{p}\right) \prod_{p\nmid ab}\left(1-\frac{2}{p^2}\right) + O\left(x^{\frac{3}{4}}(ab)^{-\frac{1}{2}}2^{\omega(ab)}\right) +$$

$$+ \left(\frac{x}{b}\right)^{\frac{1}{2}} + \left(\frac{x}{a}\right)^{\frac{1}{2}}\frac{1}{b}\Big).$$

PROOF OF LEMMA 1. Let H be a parameter which satisfies $1 \le H \le (x/b)^{\frac{1}{2}}$. Observe that the number of solutions in natural numbers u and v of the equation $uu_0 - vv_0 = 1$, $vv_0 \le x$, $(u_0,v_0) = 1$, $u_0,v_0 \in \mathbf{N}$ is uniformly $x/(u_0v_0) + O(1)$. Using then $\mu^2(l) = \sum_{mc^2=l} \mu(c)$ we have, for S defined by (2.5),

$$S = \sum_{\substack{c^2m\le x/b,\,(c,ab)=1,\,(m,ab)=1,\\ mbc^2=ka-1,\,(k,a)=1}} \mu(c)\mu^2(k)$$

$$= \sum_{c\le (x/b)^{\frac{1}{2}},\,(c,ab)=1} \mu(c) \sum_{\substack{k\le (x+1)/a,\,(k,abc^2)=1,\\ ka=mbc^2+1,\,(m,b)=1}} \mu^2(k)$$

$$= \sum_{c\le H,\,(c,ab)=1} \mu(c) \sum_{\substack{k\le (x+1)/a,\,(k,abc^2)=1,\\ ka=mbc^2+1,\,(m,b)=1}} \mu^2(k) +$$

$$+ O\left(\sum_{H\le c\le (x/b)^{\frac{1}{2}}} \sum_{k\le (x+1)/a,\,k\equiv a' (\mathrm{mod}\ bc^2)} 1\right)$$

$$(a' = a'(b,c))$$

$$= \sum_{c\le H,(c,ab)=1} \mu(c) \sum_{d\le((x+1)/a)^{\frac{1}{2}},(d,abc)=1} \mu(d)$$

$$\times \sum_{ad^2r=mbc^2+1,\,mbc^2\le x,(m,b)=1,(r,a)=1} 1$$

$$+ O(x/(abH) + (x/b)^{\frac{1}{2}})$$

$$= \sum_{c\le H,(c,ab)=1} \mu(c) \sum_{d\le((x+1)/a)^{\frac{1}{2}},(d,abc)=1} \mu(d) \sum_{e|a} \mu(e)$$

$$\times \sum_{f|b} \mu(f) \sum_{\substack{ad^2er_1=fm_1bc^2+1,\,fm_1bc^2\le x\\(r_1,bcf)=(m_1,ade)=1}} 1$$

$$+ O(x/(abH) + (x/b)^{\frac{1}{2}}) \qquad (r = r_1e,\ m = m_1f)$$

$$= \sum_{c\le H,(c,ab)=1} \mu(c) \sum_{d\le((x+1)/a)^{\frac{1}{2}},(d,abc)=1} \mu(d)$$

$$\times \left(\prod_{p|ab} (1-\frac{1}{p}) \frac{x}{abc^2d^2} + O(2^{\omega(ab)}) \right)$$

$$+ O(x/(abH) + (x/b)^{\frac{1}{2}})$$

$$= \frac{x}{ab} \prod_{p|ab} (1-\frac{1}{p}) \sum_{c=1,(c,ab)=1}^{\infty} \mu(c)c^{-2} \sum_{d=1,(d,abc)=1}^{\infty} \mu(d)d^{-2}$$

$$+ O(\frac{x}{abH}) + O((\frac{x}{b})^{\frac{1}{2}}) + O(H(\frac{x}{a})^{\frac{1}{2}}2^{\omega(ab)}) + O((\frac{x}{a})^{\frac{1}{2}}\frac{1}{b}).$$

Now we choose $H = x^{\frac{1}{4}}b^{-\frac{1}{2}}$, so that the condition $H \le (x/b)^{\frac{1}{2}}$ is obvious, and $H \ge 1$ for $b \le x^{\frac{1}{2}}$, and the above error terms are

$$\ll x^{\frac{3}{4}}(ab)^{-\frac{1}{2}}2^{\omega(ab)} + (x/b)^{\frac{1}{2}} + (x/a)^{\frac{1}{2}}b^{-1}.$$

It remains to evaluate the constant which appears in the above main term. This is equal to

$$(ab)^{-1} \prod_{p|ab}(1-p^{-1}) \sum_{c=1,(c,ab)=1}^{\infty} \mu(c)c^{-2}$$

$$\times \sum_{d=1,(d,abc)=1}^{\infty} \mu(d)d^{-2}$$

$$= (ab)^{-1} \prod_{p|ab}(1-p^{-1}) \prod_{p\nmid ab}(1-p^{-2})6\pi^{-2}$$

$$\times \sum_{c=1,(c,ab)=1}^{\infty} \mu(c)c^{-2} \prod_{p|c}(1-p^{-2})^{-1}$$

$$= 6(\pi^2 ab)^{-1} \prod_{p|ab}(1-p^{-1}) \prod_{p\nmid ab}(1-p^{-2})(1-p^{-2}(1-p^{-2})^{-1})$$

$$= 6(\pi^2 ab)^{-1} \prod_{p|ab}(1-p^{-1}) \prod_{p\nmid ab}(1-2p^{-2}),$$

so that the proof of Lemma 1 is complete. For $x^{\frac{1}{2}} < b \le x$ in most cases the trivial bound

$$S \ll \frac{x}{ab} + 1 \tag{2.7}$$

suffices. (2.7) follows from

$$S \le \sum_{1\le x/b,\, lb\equiv -1 \pmod a,\ (a,b)=1} 1 \le \sum_{1\le x/b,\, l\equiv l'(\mathrm{mod}\ a)} 1 = \frac{x}{ab} + O(1),$$

where $l' = l'(b)$.

PROOF OF THEOREM 1 AND THEOREM 2. Having at our disposal Lemma 1 it will be a relatively simple matter to prove both Theorem 1 and Theorem 2. Let $s(n)$ be the squarefull part of n, let q and s denote squarefull and squarefree numbers respectively, and let H be a parameter which satisfies $1 \le H \le x^{\frac{1}{2}}$. Then we have

$$\sum_{n\le x,\, f(n)=g(n+1)} 1 = \sum_{n\le x,\, f(n)=g(n+1),\, s(n)\le H} 1 + \sum_{n\le x,\, f(n)=g(n+1),\, s(n)>H} 1$$

$$= \sum_{n\le x,\, f(n)=g(n+1),\, s(n)\le H} 1 + O\Big(\sum_{H\le s\le x} \sum_{q\le x/s} 1 \Big)$$

$$= \sum_{n\le x,\, f(n)=g(n+1),\, s(n)\le H} 1 + O(xH^{-\frac{1}{2}})$$

$$= \sum_{n\le x,\, f(n)=g(n+1),\, s(n)\le H,\, s(n+1)\le H} 1 + O(xH^{-\frac{1}{2}})$$

$$= \sum_{s_1, s_2 \le H,\, (s_1, s_2)=1,\ f(s_1)=g(s_2)} \ \sum_{q_2 s_2 - q_1 s_1 = 1,\ q_1 s_1 \le x,\, (q_1, s_1)=(q_2, s_2)=1} 1 + O(xH^{-\frac{1}{2}}).$$

In the last expression the inner sum may be estimated by Lemma 1. Hence (2.6) gives ($s_1 \le H \le x^{\frac{1}{2}}$)

$$\sum_{n\le x,\, f(n)=g(n+1)} 1 = \frac{6x}{\pi^2} \sum_{\substack{s_1,s_2\le H,\,(s_1,s_2)=1\\ f(s_1)=g(s_2)}} \frac{1}{s_1 s_2}$$

$$\prod_{p\mid s_1 s_2}\left(1-\frac{1}{p}\right)\prod_{p\mid s_1 s_2}\left(1-\frac{2}{p^2}\right) \tag{2.8}$$

$$+ O(xH^{-\frac12}) + O\left(\sum_{s_1,s_2\le H} x^{\frac12} s_1^{-\frac12}\right) +$$

$$+ O\left(\sum_{s_1,s_2\le H} x^{\frac34} 2^{\omega(s_1)} s_1^{-\frac12} 2^{\omega(s_2)} s_2^{-\frac12}\right).$$

But if s denotes squarefull numbers, then by easy elementary arguments we have, as $x\to\infty$,

$$\sum_{s\le x} 1 \sim \frac{\zeta(3/2)}{\zeta(3)} x^{\frac12}, \quad \sum_{s\le x} 2^{\omega(s)} s^{-\frac12} \ll \log^2 x, \quad \sum_{s>x} s^{-1} \ll x^{-\frac12}. \tag{2.9}$$

Using (2.9) in (2.8) we obtain

$$\sum_{n\le x,\, f(n)=g(n+1)} 1 = Ax + O(xH^{-\frac12}) + O(x^{\frac12}H^{\frac12}\log x) + O(x^{\frac34}\log^4 x). \tag{2.10}$$

If we choose $H = x^{\frac12}$, then (2.10) immediately gives (2.1).

The proof of Theorem 2 is completely analogous. We have

$$\sum_{n\le x} f(n)g(n+1) = \sum_{n\le x,\, s(n)\le H,\, s(n+1)\le H} f(n)g(n+1) + \tag{2.11}$$

$$+ O(x^{1+\varepsilon}H^{-\frac12})$$

$$= \sum_{s_1,s_2\le H,(s_1,s_2)=1} f(s_1)g(s_2) \sum_{\substack{q_2s_2-q_1s_1=1,\\ q_1s_1\le x,(q_1,s_1)=(q_2,s_2)=1}} 1$$

$$+ O(x^{1+\varepsilon}H^{-\frac{1}{2}}),$$

where we used $f(n) \ll n^{\varepsilon}, g(n) \ll n^{\varepsilon}$ in estimating the error term. Using again Lemma 1 and proceeding as in the previous proof we obtain (2.3) and (2.4).

3. APPLICATIONS

As already remarked, several common arithmetic functions such as $a(n)$, $\Omega(n) - \omega(n)$ and $\mu^2(n)$ (the characteristic function of squarefree numbers) clearly belong to $\mathcal{B}$. It was also remarked that $f,g \in \mathcal{B}$ implies $f \cdot g \in \mathcal{B}$ and $f^{\alpha} \in \mathcal{B}$ for α a natural number; however for Theorem 2 we may take even $\alpha \in \mathrm{Re}$, since the proof obviously works for the sum $\sum_{n\le x} f^{\alpha_1}(n)g^{\alpha_2}(n+1)$ if $f,g \in \mathcal{B}$, $\alpha_1,\alpha_2 \in \mathrm{Re}$ and f,g, are positive for all n. Thus as corollaries of Theorem 2 we have

$$(3.1) \qquad \sum_{n\le x} a(n)(\Omega(n+1) - \omega(n+1)) = Cx + O(x^{\frac{3}{4}+\varepsilon}) \qquad (C > 0),$$

$$(3.2) \qquad \sum_{n\le x} a^r(n)a^s(n+1) = C_{r,s}x + O(x^{\frac{3}{4}+\varepsilon})$$

with $C_{r,s} > 0$ and $r,s \in \mathrm{Re}$ fixed. Hence by the binomial

theorem (3.2) implies

$$(3.3) \qquad \sum_{n\le x} (a(n) - a(n+1))^{2m} = C_m x + O(x^{\frac{3}{4}+\varepsilon})$$

with $C_m > 0$ and $m \in \mathbf{N}$ fixed. From Theorem 1 we have

$$(3.4) \qquad \sum_{n\le x, a(n)=a(n+1)} 1 = D_1 x + O(x^{\frac{3}{4}}\log^4 x),$$

$$(3.5) \qquad \sum_{n\le x, a(n)=\Omega(n+1)-\omega(n+1)} 1 = D_2 x + O(x^{\frac{3}{4}}\log^4 x),$$

where $D_1, D_2 > 0$, the latter formula being true since $a(s_1) = \Omega(s_2) - \omega(s_2)$ has the solution $s_1 = p_1^2$, $s_2 = p_2^3$ (p's primes). The method of proof of Theorem 1 works also for sums like $\sum_{n\le x, rf(n)=g(n+1)} 1$, where $f, g \in \mathcal{B}$ and $r > 0$ is given rational number. It would be too long to state explicitly all interesting applications of our theorems. We mention only one more, namely

$$(3.6) \qquad \sum_{n\le x} \mu^2(n)\mu^2(n+1) = Dx + O(x^{\frac{3}{4}+\varepsilon}), \quad D = \prod_p (1 - 2p^{-2}),$$

and the sum in (3.6) is interesting, since it represents the number of $n \le x$ such that both n and $n+1$ are squarefree. However, for this particular problem much better error terms are known: $O(x^{2/3+\varepsilon})$ is due to L. Carlitz [1], $O(x^{2/3}\log^{4/3} x)$ to L. Mirsky [21], [22], $O(x^{2/3}\log^{2/3} x)$ to R.R. Hall [8], and finally $O(x^{7/11}\log^7 x)$ was proved

recently by D.R. Heath-Brown [10]. Likewise, the error terms in (3.2) and (3.3) may be replaced by $O(x^{2/3+\varepsilon})$. This follows from Th. 1 of L. Mirsky [24], but his method requires the functions in question to be sub-multiplicative, hence it cannot give e.g. (3.1) nor, in general, Th.2, and it cannot be used at all for the sum in Theorem 1.

There are several more general sums than the ones in (2.1) and (2.2) which may be also evaluated by methods similar to those used in proving Theorem 1 and Theorem 2. Consider, for example, $\sum_{n\le x} f(n)h(n+1)$, where $f(n) \in \mathbf{B}$, and $h(n)$ is a positive, integer-valued arithmetic function for which only $h(n) \ll n^{\varepsilon}$ is supposed to hold (so that $h(n)$ is not necessarily a s-function). If $1 \le H \le x^{\frac{1}{2}}$ is a parameter, than we have

$$(3.7)\qquad \sum_{n\le x} f(n)h(n+1) = \sum_{n\le x,\, s(n)\le H} f(n)h(n+1) + O(x^{1+\varepsilon}H^{-\frac{1}{2}})$$

$$= \sum_{s\le H} f(s) \sum_{q\le x/s,\,(q,s)=1} h(qs+1) + O(x^{1+\varepsilon}H^{-\frac{1}{2}})$$

$$= \sum_{s\le H} f(s) \sum_{\substack{d\le (x/s)^{\frac{1}{2}},\\ (d,s)=1}} \mu(d) \sum_{\substack{m\le x/(sd^2),\\ (m,s)=1}} h(msd^2+1) + O(x^{1+\varepsilon}H^{-\frac{1}{2}})$$

$$= \sum_{s\le H} f(s) \sum_{d\le H^{\frac{1}{2}},\,(d,s)=1} \mu(d) \sum_{\substack{m\le x/(sd^2),\\ (m,s)=1}} h(msd^2+1) +$$

$$+ O(x^{1+\varepsilon}H^{-\frac{1}{2}}) + O(Hx^{\varepsilon})$$

$$= \sum_{s\le H} f(s) \sum_{d\le H^{\frac{1}{2}},(d,s)=1} \mu(d) \sum_{\delta|s} \mu(\delta) \sum_{k\le x,k\equiv 1(\mathrm{mod}\ sd^2\delta)} h(k) +$$

$$+ O(x^{1+\varepsilon}H^{-\frac{1}{2}}) + O(Hx^{\varepsilon}),$$

where as before q and s denote squarefree and squarefull numbers, respectively. Therefore if we can find an asymptotic formula for

$$(3.8) \qquad H(x,r) = \sum_{n\le x,n\equiv 1(\mathrm{mod}\ r)} h(n) \qquad (r = ds\delta^2),$$

which is uniform in $r = r(x)$ for a certain range, then inserting (3.8) in (3.7), simplifying and choosing H optimally we obtain an asymptotic formula for the summatory function of $f(n)h(n+1)$. As an example, consider $h(n) = d(n)$, the number of divisors of n. It was proved by D.R. Heath-Brown [9] that

$$(3.9) \qquad \sum_{n\le x,n\equiv 1(\mathrm{mod}\ r)} d(n) = \frac{x}{r^2}(A(r,1)(\log\frac{x}{r^2} + 2\gamma - 1) + 2B(r,1)) +$$

$$+ O(x^{1/3+\varepsilon})$$

uniformly for $1 \le r \le x^{2/3}$, where γ is Euler's constant and

$$A(r,1) = \sum_{d|r} d\mu(\frac{r}{d}) \ll rx^{\varepsilon}, \quad B(r,1) = \sum_{d|r} d\mu(\frac{r}{d})\log d \ll rx^{\varepsilon}.$$

For $r = sd^2\delta$, $s \le H$, $d^2 \le H, \delta \le H$ the condition $r \le x^{2/3}$ is satisfied if $H = x^{2/9}$, whence from (3.7) and (3.9) we obtain

$$(3.10) \qquad \sum_{n\le x} f(n)d(n+1) = C_1 x \log x + C_2 x + O(x^{8/9+\varepsilon}).$$

In this formula, which appears to be new (and gives (1.5) as a special case), $f \in B$, $C_1 \ge 0$ and C_2 are two constants which may be explicitly evaluated. The analogous problem with $d(n)$ replaced by $d_3(n)$ may be considered if one appeals to the recent result of J.B. Friedlander and H. Iwaniec [7] concerning the asymptotic formula for $\sum_{n\le x, n\equiv a(\mathrm{mod}\ q)} d_3(n)$, $(a,q)=1$. A corresponding formula for $H(x,r)$ in (3.8) when $h(n) = \omega(n)$ or $\Omega(n)$ may be obtained by the methods of H. Delange [2], and in this case the error term would be uniform for $1 \le r \le \log^C x$, $C > 0$ any fixed number. This would give, for $f \in B$,

$$(3.11) \qquad \sum_{n\le x} f(n)\omega(n+1) = D_1 x \log\log x + D_2 x + O(x/\log x)$$

where $D_1 \ge 0$ and D_2 may be explicitly evaluated. In (3.11) one may consider $\omega^k(n+1)$ for any fixed $k \in \mathbf{N}$ instead of $\omega(n+1)$ only. In this case the right-hand side of (3.11) would contain as the main term x times a polynomial of degree k in $\log\log x$.

One may also consider the sum

$$(3.12) \qquad \sum_{n\le x} f(n)g(n+k)$$

where $f,g \in \mathbf{B}$ and $k > 1$. In fact, k may be assumed to be any fixed natural number, and even $k = k(x)$ may be interesting. It is possible to evaluate the general sum appearing in (3.12) by proceeding as in (3.7). In this way one is led to the estimation of the sums

$$G(x;r,l) = \sum_{n\le x,\, n\equiv l \pmod r} g(n)$$

where $(l,r) = 1$ does not have to hold, and consequently the estimation of $G(x;r,l)$ may be technically difficult. The same applies to the estimation of the sum

$$(3.13) \qquad S_k(x) = \sum_{n\le x} f_1(n+\ell_1)f_2(n+\ell_2)\dots f_k(n+\ell_k),$$

where $f_1, \dots, f_k \in B$, $0 \le \ell_1 \le \dots \le \ell_k$ are fixed integers. This sum would be asymptotic to Cx, $C = C(f_1,\dots,f_k,\ell_1,\dots,\ell_k) \ge 0$, and its evaluation would reduce to $S_{k-1}(x)$ for n in a certain residue class. Under certain conditions which include multiplicativity or sub-multiplicativity of the f_i's, this follows from the works of P. Erdős [3] and L. Mirsky [24], respectively, and the latter gives a good error term. But none of these apply to the case when the f_i's are s-functions. Also one should be careful in treating (3.13), since in the general case it

may well turn out that $C = C(f_1,\dots,\ell_k)$ is zero, or even that the whole sum under consideration is zero. As an example, we recall L. Mirsky's formula (1.13), but note that identically

$$\sum_{n\le x} \mu^2(n)\mu^2(n+1)\mu^2(n+2)\mu^2(n+3) = 0,$$

since one of any four consecutive integers must be divisible by four, and $\mu(4m) = 0$ for any $m \ge 1$. For a generalization of (3.13) when $f_j = \mu^2$, see R.R. Hall [8].

4. THE DISTRIBUTION OF VALUES OF a(n)

As in 1. we let $C(x)$ and $D(x)$ denote the number of distinct values of $a(n)$ for $n \le x$ and the number of $n \le x$ such that $n = a(m)$ for some m, respectively. An unconditional proof of the formulas in (1.9) seems quite difficult, but it seems reasonable to expect that $\lim_{x\to\infty} C(x)/D(x) = 0$ may be at least proved. This follows from

THEOREM 3. For $x \ge x_0$

$$D(x) \ge \frac{1}{3}C(x)\log\log x. \tag{4.1}$$

PROOF OF THEOREM 3. Let $n_1 = a(k_1),\dots,n_t = a(k_t)$ $(k_j \le x)$ be the distinct values of $a(n)$ for $n \le x$. Then $t = C(x)$, and from (1.4) it follows that

$$n_j \le \exp(\log x/(2\log\log x)), (x \ge x_0;\ j=1,\dots,t).$$

Put

$$m_{j,r} = k_j(q_1 q_2 \dots q_{ru})^2,$$

where $q_1, q_2, \dots$ are distinct primes not dividing any of the k_j's (e.g. take $q_1 > x$ for $l = 1,2,\dots$), $r \ge 1$ is an integer and $u = [\log x/(\log 2 \log\log x)]$. Thus

$$a(m_{j,r}) = a(k_j)a(q_1^2)\dots a(q_{ru}^2) = n_j(2^u)^r \le x$$

for $j = 1,\dots,t$ and $1 \le r \le [\frac{1}{2}\log\log x]$, so that there are at least

$$[\tfrac{1}{2}\log\log x]t \ge \tfrac{1}{3} C(x) \log\log x$$

numbers $a(m_{j,r})$ for $x \ge x_0$, and (4.1) follows if they are all distinct. Suppose that this is not true. Then if

$$n_j 2^{ru} = n_k 2^{su} \tag{4.2}$$

for $s > r$, we have for $x \ge x_0$

$$\exp(\log x/(2\log\log x)) \ge n_j/n_k =$$

$$= 2^{u(s-r)} \ge 2^u \ge \exp(3\log x/(4\log\log x)),$$

which is a contradiction. It follows that in (4.2) we have $s = r$, hence $j = k$, and (4.1) is proved.

Note that if (1.9) is true, then $D(x)$ is roughly $C(x)$ to the power $\log^{1/6} x$, which is incomparably stronger than (4.1). On the other hand, practically the only

property of $a(n)$ that was used in the above proof was the bound (1.4). Hence an analogous result may be easily formulated for a wide class of multiplicative, prime-independent functions which take natural numbers as values and satisfy a growth condition similar to (1.4).

To obtain lower bounds for $C(x)$ we proceed as follows. Let $t,r \geq 1$ be integers (to be suitably chosen later), and let p_n denote the n-th prime. Consider numbers of the form

$$(4.3) \qquad n = (p_1 \cdots p_{j_1})^{k_1} (p_{r+1} \cdots p_{r+j_2})^{k_2} \cdots$$

$$\cdots (p_{r(t-1)+1} \cdots p_{r(t-1)+j_t})^{k_t},$$

where each j_l $(l = 1,\ldots,t)$ takes all possible values $j_l = 1,2,\ldots,r$ and $1 \leq k_1 < k_2 < \ldots < k_t$ are suitably chosen integers. By the prime number theorem $p_n = (1+o(1))n \log n$ as $n \to \infty$ and $\theta(x) = \sum_{p \leq x} \log p = x + o(x)$ as $x \to \infty$, hence for rt large

$$n \leq \exp(k_t \theta(p_{rt})) \leq \exp(2k_t rt \log(rt)) \leq \exp(\log x) = x$$

if r,t and k_t satisfy

$$(4.4) \qquad 2k_t rt \log(rt) \leq \log x \qquad (x \geq x_0).$$

Moreover,

$$(4.5) \qquad a(n) = P^{j_1}(k_1)P^{j_2}(k_2)\ldots P^{j_t}(k_t) ,$$

and we wish all the numbers of the form (4.5) to be distinct. Therefore the sequence $k_1 < \ldots < k_t$ should be chosen in such a way that

$$(4.6) \qquad a(n_1) = P^{j_1}(k_1)\ldots P^{j_t}(k_t) = P^{l_1}(k_1)\ldots P^{l_t}(k_t) = a(n_2)$$

implies $n_1 = n_2$ for $1 \le j_m, l_n \le r$, $1 \le m,n \le t$. If (4.4) and the last condition are satisfied, then there are r^t different numbers of the form (4.3), and it follows that

$$(4.7) \qquad C(x) \ge r^t .$$

Hence the larger tlog r is, the better our lower bound for C(x) will be, and therefore k_t (as a function of t) should be as small as possible. One may think of the numbers k_j as the elements of the (minimal) basis of the multiplicative semigroup generated by P(1), P(2), P(3), ..., so that k_j is the j-th element of the basis. In this context D(x) represents the number of distinct elements of this semigroup which do not exceed x. To obtain a specific, unconditional lower bound for C(x) we shall use the following

LEMMA 2. (A. Schinzel) If $\omega(n)$ is the number of distinct prime factors of n, then

$$\lim_{n\to\infty} \omega\Big(\prod_{j=1}^{n} P(j)\Big) = \infty \quad . \tag{4.8}$$

PROOF OF LEMMA 2. For the partition function we shall use the well-known asymptotic formula (see e.g. M. Knopp [18], p. 90)

$$P(n) = \frac{1}{4\sqrt{3}} \cdot \frac{e^{a\lambda_n}}{n - 1/24} \left(1 - \frac{1}{a\lambda_n}\right) + O(e^{5a\lambda_n/8}) , \tag{4.9}$$

where $\lambda_n = (n - 1/24)^{1/2}$ and $a = \pi(2/3)^{1/2}$. We suppose that the primes $q_1,\ldots,q_r$ constitute the prime factors of P(n) for every $n \geq 2$. We shall use a result of R. Tijdeman [30], which says that there exists a constant $C < 0$ such that if the numbers A and B are composed only of $q_1,\ldots,q_r$ and $|A - B| \leq A\log^C A$, then $A = B$. Let us choose two sets of positive integers $a_1,\ldots,a_k$ and $b_1,\ldots,b_k$ such that

$$\sum_{j=1}^{k} a_j^m = \sum_{j=1}^{k} b_j^m$$

for $m = 1,2,\ldots, [c/2]$, but

$$\sum_{j=1}^{k} a_j^{[c/2]+1} \neq \sum_{j=1}^{k} b_j^{[c/2]+1} \quad .$$

Using (4.9), Taylor's expansion and simplifying the resulting expressions we obtain

$$(4.10) \qquad \prod_{j=1}^{k} P(n+a_j) = \prod_{j=1}^{k} P(n+b_j)(1+0(n^{-1/2-[c/2]}))$$

and also

$$(4.11) \qquad \prod_{j=1}^{k} P(n+a_j) = \prod_{j=1}^{k} P(n+b_j)(1+\Omega(n^{-1/2-[c/2]})).$$

Putting in Tijdeman's theorem

$$A = \prod_{j=1}^{k} P(n+a_j), \quad B = \prod_{j=1}^{k} P(n+b_j)$$

we find from (4.10)

$$A - B \ll A(\log A)^{-2[c/2]-1},$$

which yields A = B. However, this contradicts (4.11), so (4.8) must hold.

From Lemma 2 it follows that there exist arbitrarily large t and integers $2 = k_1 < k_2 < k_t$ such that there exist primes $2 = q_1 < q_2 < \ldots < q_t$ with the property that each q_j divides $P(k_j)$ but does not divide any $P(k_l)$ for $l < j$, i.e. $\lim_{t\to\infty} k_t = \infty$. We shall take $t = [A] + 1$ (where $A > 0$ is any fixed constant), $r = [C\log x/\log\log x]$, $C = 1/(10k_t t)$. Then (4.4) clearly holds, and all numbers of the form (4.5) are distinct. Namely, if (4.6) holds, we must have first $j_t = l_t$

(since q_t does not divide $P(k_m)$ for $1 \le m \le t-1$), likewise $j_{t-1} = l_{t-1}, \ldots$, until finally we obtain $j_1 = l_1$, that is, $n_1 = n_2$. Consequently (4.7) gives immediately

THEOREM 4. For any fixed $A > 0$ and $x \ge x_0(A)$

$$C(x) > (\log x)^A . \tag{4.12}$$

It is clear that any non-trivial bound of the form $k_t \le g(t)$, where $g(t)$ is a positive, increasing function tending to ∞, would improve (4.12). For example, if we had $k_t \ll e^{ct}$ $(c > 0)$, then by the foregoing argument it would follow that $C(x) > \exp(B(\log\log x)^2)$ for some $B > 0$. Actually, it seems not unreasonable to expect a drastically better bound for k_t to be true, namely

$$k_t \ll t^{1+\varepsilon} , \tag{4.13}$$

which is (up to ε) best possible. Proving (4.13) seems quite difficult, but perhaps it is not hopeless to expect that $k_t \ll t^B \log^C t$ may be proved with some $B \ge 1$, $C \ge 0$. If this were so, then taking $r = 2$ in our construction we would obtain

$$n \le \exp(2k_t r \log(rt)) \le \exp(D_1 t^{B+1} \log^{C+1} t) \le x$$

$$(D_1 > 0,\ x \ge x_0)$$

for

$$t = [D_2(\log x)^{1/(B+1)}(\log\log x)^{-(C+1)/(B+1)}],$$

$$(D_2 > 0)$$

which exists by Lemma 2. (Note the principle of the construction: if we have a poor bound for k_t, take r as large as possible; if we have a good bound for k_t, take r = 2, i.e. as small as possible). Then (4.7) gives

$$(4.14) \qquad C(x) \geq r^t = 2^t \gg \exp(D_3(\log x)^{1/(B+1)}(\log\log x)^{-(C+1)/(B+1)})$$

for some $D_3 > 0$. In this case the numbers of the form (4.5) are all distinct, and in fact (4.5) also gives

$$a(n) \leq P^{rt}(k_t) \leq \exp(C\, k_t^{1/2} rt) \leq$$

$$\leq \exp(C_2 t^{(B+2)/2} \log^{C/2} t) \leq \exp(\log x) = x$$

for some C_1, $C_2 > 0$ if r = 2 and

$$t = [D_4(\log x)^{2/(B+2)}(\log\log x)^{-C/(B+2)}], (D_4 > 0).$$

Note that we used here an upper bound for the partition function (follows easily from (4.9)), hence an intrinsic property of a(n). With this t the numbers of the form (4.5) are all counted by D(x), and we obtain

$$(4.15) \qquad D(x) \geq 2^t \gg \exp(D_5(\log x)^{2/(B+2)}(\log\log x)^{-C/(B+2)})$$

$$(D_5 > 0).$$

In particular, if we recall that (1.7) - (1.9) hold unconditionally, then from (4.13) - (4.15) we obtain

THEOREM 5. If the bound (4.13) holds, then as $x \to \infty$

$$C(x) = \exp((\log x)^{1/2+o(1)}),$$

$$D(x) = \exp((\log x)^{2/3+o(1)}).$$

This means that if the conjecture (4.13) is true, then (up to the evaluation of the $o(1)$ terms) we have determined asymptotically the order of magnitude of $C(x)$ and $D(x)$. It is also worth remarking that the above procedure for bounding $C(x)$ can be carried over to count distinct values of other multiplicative, prime-independent, positive, integer-valued functions $f(n)$. Instead of trying to obtain a general result, we shall consider the familiar function $f(n) = d_k(n)$. In this case

$$g(\alpha) = d_k(p^\alpha) = \frac{(\alpha + 1)(\alpha + 2)\ldots(\alpha + k - 1)}{(k - 1)!}$$

plays the role that $P(n)$ had for $a(n)$. Now q divides $g(q - 1)$ for $q(> k-1)$ prime, and for almost all q $g(q - m)$ $(m > 1)$ is not divisible by q. Hence in the above notation $k_t \ll t^B \log^C t$ with $B = C = 1$ for $d_k(n)$. If we recall the classical Hardy-Ramanujan formula for the number of integers of the form $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$

($a_1 \geq a_2 \geq \ldots \geq a_r$, p_j the j-th prime) not exceeding x, used in majorizing C(x) as in (1.8), then from (4.14) with B = C = 1 we obtain unconditionally

$$(4.16) \qquad \exp(E_1(k)(\log x)^{1/2}/\log\log x) \ll C(x) \ll$$

$$\ll \exp(E_2(\log x/\log\log x)^{1/2})$$

with $E_1(k) > 0$, $E_2 = 2\pi 3^{-1/2} + \varepsilon$. This seems new for $k > 2$, but is was already mentioned (see (1.12)) that P. Erdős and L. Mirsky [5] proved a sharper result than (4.16) for k = 2. It is plausible to conjecture that for $d_k(n)$ ($k \geq 2$ fixed) one has, as $x \to \infty$,

$$C(x) = \exp((E(k) + o(1))(\log x)^{1/2}/\log\log x)$$

$$(E(k) > 0).$$

In this case the function D(x) is much easier to handle. For k = 2 one has trivially D(x) = x + O(1) (since n = d(m) has a solution for every $n \geq 1$), and for $k > 2$ it is not difficult to show that D(x) is of the order $x^{1/(k-1)+o(1)}$.

5. THE VALUES OF a(n) ON LONG BLOCKS OF CONSECUTIVE INTEGERS

In this section we shall consider the values $a(n+1)$, $a(n+2)$, ... on "long" blocks of consecutive integers. More precisely, we shall suppose $x \le n \le 2x$ and will try to find two functions $k = k(x)$ and $t = t(x)$, as large as possible, such that $a(n+1) = \ldots = a(n+k)$ for many n and such that the values $a(n+1)$, ..., $a(n+t)$ are all distinct for many n. Analogous problems may be of course considered for other common arithmetic functions, such as $d_k(n)$ for instance. The first problem is very difficult already for $d(n) = d_2(n)$, and it is known that

$$x/\log^7 x \ll \sum_{n\le x, d(n)=d(n+1)} 1 \ll x(\log\log x)^{-1/2}.$$

The lower bound is due to D.R. Heath-Brown [11], and the upper bound to P. Erdős et al. [6] (A. Hildebrand very recently announced in [14] the lower bound $x(\log\log x)^{-3}$). Nothing non-trivial seems to be known about integers n for which $d(n) = d(n+1) = d(n+2)$ etc. On the other hand, P. Erdős and L. Mirsky [5] showed that the number of $x \le n \le 2x$ such that the values $d(n+1)$, ..., $d(n+t)$ are all distinct is $\gg x^{1/2}$ if $t = [C(\log x)^{1/2}/\log\log x]$ with

a suitable $C > 0$. We are going to prove the same result for general $d_k(n)$ by a method which, in the case of $a(n)$, gives the result with $t = [C(\log x/\log\log x)^{1/2}]$. We shall also be able to find very long blocks of consecutive integers where the values of $a(n)$ are all equal. This is quite a contrast with the case of $d_k(n)$, and is essentally due to the fact that $a(n)$ is an s-function, that is, $a(q) = 1$ if q is squarefree. Our results are

THEOREM 6. There exist at least $x^{1/2}$ numbers n from $[x,2x]$ such that

$$a(n + 1) = a(n + 2) = \ldots = a(n + k),$$

$$k = \left[\frac{\log x \log\log\log x}{40(\log\log x)^2}\right]$$

THEOREM 7. There exist at least $x^{1/2}$ numbers n from $[x,2x]$ such that for a suitable $C > 0$ the values $a(n + 1), a(n + 2), \ldots, a(n + t)$ are all distinct for

$$t = [C(\log x/\log\log x)^{1/2}] .$$

PROOF OF THEOREM 6. If k is as in Theorem 6, then we shall find k integers $n+1,n+2,\ldots,n+k$ which all have the same pattern for at least $x^{1/2}$ numbers n from

[x,2x]. By this we mean that

$$(5.1) \qquad n + i = p_{i,1}^{\alpha_1} p_{i,2}^{\alpha_2} \cdots p_{i,R}^{\alpha_R} l_i \qquad (i=1,2,\ldots,k),$$

where the p_i's are distinct primes not dividing l_i, l_i is squarefree, $2 \le \alpha_1 \le \alpha_2 \le \ldots \le \alpha_R$, and we say that $(\alpha_1,\alpha_2,\ldots,\alpha_R)$ is the pattern of $n + i$. From (5.1) it follows that

$$a(n + i) = P(\alpha_1)P(\alpha_2)\ldots P(\alpha_R) \qquad (i=1,2,\ldots,k),$$

and since the right-hand side here does not depend on i, we have $a(n+1) = a(n+2) = \ldots = a(n+k)$ and Theorem 6 follows. Note that this construction does not work for $d(n)$, since

$$d(n + i) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_R + 1)2^{\omega(l_i)}$$

depends on i. Therefore our problem is reduced to the purely arithmetic problem of finding long blocks of consecutive integers with the same pattern, which seems to be a problem interesting in itself. First we define (fix) the pattern $(\alpha_1,\alpha_2,\ldots,\alpha_R)$ as follows. Note that if $2^a \le k < 2^{a+1}$, i.e. if $a = [\log k/\log 2]$, then $\alpha_R = [\log k/\log 2]$ and this occurs with multiplicity one in the pattern. The number 2 occurs among the α_r's j_1 times if j_1 is defined by

$$2^2 3^2 \ldots p_{j_1}^2 \le k < 2^2 3^2 \ldots p_{j_1}^2 p_{j_1+1}^2 ,$$

where p_m is the m-th prime. In general, for a given r such that $2 \le r \le \log k/\log 2$, the number r occurs in the pattern j_r times, where j_r (≥ 1) is defined by

$$(5.2) \qquad p_1^r p_2^r \ldots p_{j_r}^r \le k < p_1^r p_2^r \ldots p_{j_r}^r p_{j_r+1}^r .$$

Therefore, roughly speaking, the numbers occurring in the pattern will represent the union of all possible exponents of squarefull numbers not exceeding k. Small α_r's will appear in the pattern with a large multiplicity, and large α_r's with a small one. Namely from (5.2) and the prime number theorem we have, for $2 \le r \le g(k)$, $g(k) = o(\log k/\log\log k)$ as $k \to \infty$,

$$(5.3) \qquad j_r = \frac{(1 + o(1))\log k}{r \log\log k} .$$

In general, for $r_0 \le r \le \log k/\log 2$, (5.2) implies by estimates from elementary prime number theory

$$(5.4) \qquad j_r \le \frac{5 \log k}{r \log(\frac{\log k}{r} + 1)} .$$

Our construction gives then the precise pattern of numbers of the form (5.1). Further, for $p_j \le k^{1/2}$ we

define c_j (≥ 2) as the integer for which $p_j^{c_j-1} \leq k < p_j^{c_j}$, and we denote by $J = \pi(k^{1/2})$ the largest j such that $p_j \leq k^{1/2}$. We require first

$$(5.5) \qquad n \equiv p_1^{c_1} p_2^{c_2} \ldots p_J^{c_J} \pmod{p_1^{c_1+1} p_2^{c_2+1} \ldots p_J^{c_J+1}} .$$

Next we require that, for $i = 1,\ldots,k$,

$$(5.6) \qquad n + i \equiv p_{i,1}^{\alpha_1} p_{i,2}^{\alpha_2} \ldots p_{i,R}^{\alpha_R} \pmod{p_{i,1}^{\alpha_1+1} p_{i,2}^{\alpha_2+1} \ldots p_{i,R}^{\alpha_R+1}} ,$$

where $(\alpha_1,\alpha_2,\ldots,\alpha_R)$ is the pattern defined above, and the congruence conditions ensure that $p_{i,j}^{\alpha_j} \| n + i$. Here the $p_{i,j}$'s are distinct primes exceeding $k^{1/2}$, to be taken as small as possible. The congruences (5.6) are to hold if no prime powers that divide i divide also $F = p_1^{c_1} \ldots p_J^{c_J}$. If this condition is not satisfied, and if e.g. some p^β ($\beta \geq 2$) divides i and F, then the corresponding factor $p_{i,1}^\beta$ is to be omitted in (5.6). This procedure is necessary, since in view of (5.5) the numbers $n + i$ are automatically divisible by i if $i|F$, and therefore the omission of suitable $p_{i,1}^\beta$'s will ensure that the pattern $(\alpha_1,\alpha_2,\ldots,\alpha_R)$ of each $n + i$ is preserved. To elucidate this idea, take $k = 40$. Then the pattern is $(2,2,3,4,5)$, we choose $n \equiv 2^6 3^4 5^3 \pmod{2^7 3^5 5^4}$,

$$n+1 \equiv 7^2 11^2 13^3 17^4 19^5 \pmod{7^3 11^3 13^4 17^5 19^6},$$

and analogously for $n+2$ and $n+3$ we introduce 10 new consecutive primes. But since 2^2 divides $F = 2^6 3^4 5^3$, we shall have

$$n+4 \equiv p_{4,1}^2 p_{4,2}^3 p_{4,3}^4 p_{4,4}^5 \pmod{p_{4,1}^3 p_{4,2}^4 p_{4,3}^5 p_{4,4}^6},$$

similarly

$$n+32 \equiv p_{32,1}^2 p_{32,2}^2 p_{32,3}^3 p_{32,4}^4 \pmod{p_{32,1}^3 p_{32,2}^3 p_{32,3}^4 p_{32,4}^5}$$

$$n+36 \equiv p_{36,1}^3 p_{36,2}^4 p_{36,3}^5 \pmod{p_{36,1}^4 p_{36,2}^5 p_{36,3}^6},$$

and so on. Note that the moduli in (5.5) and (5.6) are all pairwise coprime, hence by the Chinese remainder theorem the system of congruences will have a unique solution modulo A(k), say. From (5.3) and (5.4) it follow that

$$R = \sum_{2 \le r \le \log k/\log 2} j_r \le 6 \log k \log\log k .$$

For each $n+i$ we introduce at most R new primes, so that A(k) is the product of at most $6k\log k\log\log k$ consecutive primes exceeding $k^{1/2}$, some of which may have exponents as large as $\log k/\log 2$. For our purpose, however, it is desirable to have A(k) as small as possible, and therefore in constructing the congruences

(5.6) we shall make the following stipulation. For numbers r appearing in the pattern $(\alpha_1,\alpha_2,\dots,\alpha_R)$ such that $2 \le r \le \varepsilon\log k/\log\log k$ (this corresponds to (5.3)), we choose the primes $p_{i,r}$ (for each $i = 1,\dots,k$) as small as possible, and then we "fill in" the larger primes for the r's appearing with smaller multiplicities (this corresponds to (5.4)). Thus for $r > \varepsilon\log k/\log\log k$ we obtain $j_r \ll_\varepsilon \log\log k$ in (5.4). Moreover we have from (5.3), as $k \to \infty$,

$$\sum_{2\le r\le \varepsilon\log k/\log\log k} j_r \le \sum_{2\le r\le \log k} \frac{(1+o(1))\log k}{r\log\log k} = (1+o(1))\log k .$$

Hence it follows, for some $C = C(\varepsilon) > 0$, that

$$A(k) \le \prod_{p\le (1+o(1))k\log k} p^{\log k/\log\log k} \cdot \prod_{p\le (6+o(1))k\log k\log\log k} p^{C\log\log k}$$

$$\le \exp\left(\frac{2\theta(2k\log k)\log k}{\log\log k} + 2C\theta(7k\log k\log\log k)\log\log k\right)$$

$$\le \exp\left(\frac{8k\log^2 k}{\log\log k}\right) \le x^{1/4}$$

if $k = [\log x\log\log\log x/(40\log\log x)^2]$ as in theorem 6. All solutions of (5.5) and (5.6) are of the form $n = A(k)m + B(k), 0 \le B(k) < A(k)$, hence there are $x/A(k) + O(1)$ such n from $[x,2x]$. It remains yet to show that at least $x^{1/2}$ of these n are of the form

(5.1) (i.e. that l_i in (5.1) is squarefree). This means that we have to omit those n which are $\equiv -i \pmod{p^2}$, $0 \le i \le k, p > A(k)$. For a fixed prime p ($> A(k)$) we omit $x/(A_k p^2) + O(1)$ numbers, since p^2 may divide only one $n + i$ for a fixed n. This is so, because if $n + i = m_i p^2$ and $n + j = m_j p^2$, then $A(k) \ge |i - j| = p^2 |m_i - m_j| \ge p^2$, which is obviously impossible. Hence the total number of omitted n's does not exceed

$$\sum_{A(k)<p\le x^{1/2}} \left(\frac{x}{A_k p^2} + O(1)\right) \ll x/A_k^2 + x^{1/2} = o(x/A_k) ,$$

consequently the number of n's such that (5.1) holds is $(1 + o(1))x/A_k > x^{1/2}$. This completes the proof of Theorem 6.

PROOF OF THEOREM 7. We shall develop first a general method, which gives the conclusion of Theorem 7 with a slightly poorer value $t = [C(\log x)^{1/2}/\log\log x]$ for a large class of arithmetical functions, including $d_k(n)$. Then we shall refine the argument in the case of $a(n)$, where we are dealing with an s-function, and obtain the full assertion of Theorem 7.

By the Chinese remainder theorem the system of congruences

$$
\begin{aligned}
n+1 &\equiv p_1^2 p_2^2 \cdots p_r^2 \pmod{p_1^3 p_2^3 \cdots p_r^3} \\
n+2 &\equiv p_{r+1}^2 p_{r+2}^2 \cdots p_{3r}^3 \pmod{p_{r+1}^3 p_{r+2}^3 \cdots p_{3r}^3} \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
n+t &\equiv p_{\frac{1}{2}t(t-1)r}^2 \cdots p_{\frac{1}{2}t(t+1)r}^2 \pmod{p_{\frac{1}{2}t(t-1)r}^3 \cdots} \\
&\qquad\qquad\qquad\qquad \cdots p_{\frac{1}{2}t(t+1)r}^3
\end{aligned} \tag{5.7}
$$

has a unique solution modulo $B = (p_1 p_2 \cdots p_{\frac{1}{2}t(t+1)r})^3$, where $r = [C\log\log x]$ with a suitable $C > 0$, which will be specified later. Thus

$$
\begin{aligned}
n+1 &= m_1 p_1^2 \cdots p_r^2, \qquad (m_1, p_1 \cdots p_r) = 1 \\
&\vdots \qquad\qquad \vdots \\
n+t &= m_t p_{\frac{1}{2}t(t-1)r}^2 \cdots p_{\frac{1}{2}t(t+1)r}^2,
\end{aligned} \tag{5.8}
$$

$$
(m_t, p_{\frac{1}{2}t(t-1)r} \cdots p_{\frac{1}{2}t(t+1)r}) = 1,
$$

and $n = Bm + A$ for some $0 \le A < B$. Moreover,

$$
B = \exp(3\vartheta(p_{\frac{1}{2}t(t+1)r})) \le \exp(\tfrac{7}{4}t^2 r \log(3t^2)) \le
$$

$$
\le \exp\left(2C_1^2 \frac{\log x}{(\log\log x)^2} C(\log\log x)^2\right) = x^{1/25}
$$

if $t = [C_1(\log x)^{1/2}/\log\log x]$ and $2C_1^2 C = 1/25$. Therefore

there are $x/B + O(1) > x^{19/20}$ solutions of (5.7) such that $x \le n \le 2x$. We wish to establish that for sufficiently many of these solutions n each m_j $(j = 1,\dots,t)$ in (5.8) has relatively few prime factors, since by the classical result of Hardy-Ramanujan loglogn is the normal order of $\Omega(n)$. By a result of J.-L. Nicolas [27] we have, uniformly for $3 \le k \le \log x/\log 2$,

$$(5.9) \qquad \sum_{n\le x,\,\Omega(n)\ge k} 1 \ll x2^{-k}\log x.$$

This means that the number of n's from $[x,2x]$ which satisfy (5.7) and (5.8) with $\Omega(m_1) > 100\log\log x$ is $\ll x/(p_1^2\dots p_r^2\log^{30}x)$, consequently the number of these n for which $\Omega(m_1) \le 100\log\log x$ is

$$\frac{x}{p_1^2\dots p_r^2}\left(1 + O\left(\frac{1}{\log^{30}x}\right)\right).$$

The n's which satisfy $n + 1 \equiv 0 \pmod{p_1^2\dots p_r^2}$ and $n + 2 \equiv 0 \pmod{p_{r+1}^2\dots p_{3r}^2}$ lie in a unique arithmetic progression modulo $p_1^2p_2^2\dots p_{3r}^2$, hence using again (5.9) it is seen that the number of n's for which both $\Omega(m_1) \le 100\log\log x$ and $\Omega(m_2) \le 100\log\log x$ is

$$\frac{x}{p_1^2\dots p_{3r}^2}\left(1 + O\left(\frac{2}{\log^{30}x}\right)\right),$$

where the 0-constant is absolute. Continuing this analysis, we finally obtain that the number of n's from [x,2x] for which (5.7) and (5.8) hold with $\Omega(m_1) \le 100\log\log x, \ldots, \Omega(m_t) \le 100\log\log x$ is equal to

$$\frac{x}{B}\left(1 + 0\left(\frac{t}{\log^{30} x}\right)\right) \ge \frac{x}{2B} > x^{1/2}$$

Let us define now the function b(n) by the relation $2^{b(n)} \| n$ (i.e., b(n) is the exponent of the highest power of 2 which divides n). We shall prove that

$$(5.10) \qquad b(a(n+1)) < b(a(n+2)) < \ldots < b(a(n+t)),$$

which implies that the values $a(n+1), \ldots, a(n+t)$ are all distinct, hence Theorem 7 is proved.

In view of (5.8) and $a(p^2) = 2$ we have

$$a(n+1) = a(m_1)a(p_1^2 \ldots p_r^2) = a(m_1)2^r,$$
$$a(n+2) = a(m_2)2^{2r}, \ldots, a(n+t) = a(m_t)2^{tr}.$$

But from (4.9) it easily follows that $a(p^\alpha) = P(\alpha) < \exp(c\alpha^{1/2})$ for $\alpha \ge 1$ and some suitable $c > 0$. Thus if the canonical decomposition of n is $n = q_1^{\alpha_1} \ldots q_k^{\alpha_k}$, then for $n \ge 1$

$$(5.11) \qquad a(n) = P(\alpha_1)\ldots P(\alpha_k) < \exp(c(\alpha_1^{1/2} + \ldots + \alpha_k^{1/2})) <$$

$$< \exp(c\Omega(n)) .$$

Hence $a(m_1) < e^{100c\log\log x} < 2^{r/4}$ if $r = [C\log\log x]$ with with $C > 1000c$, and analogously $a(m_2) < 2^{r/4}, \ldots, a(m_t) < 2^{r/4}$ for $x \geq x_0$. This implies

$$2^r \leq b(a(n+1)) \leq 2^{r+r/4} < 2^{2r} \leq b(a(n+2)) \leq 2^{2r+r/4} <$$

$$< 2^{3r} \leq \ldots < 2^{tr} \leq b(a(n+t)),$$

proving (5.10) and completing the proof of the weaker version of Theorem 7.

Analyzing the above proof it becomes clear that the most important property of $a(n)$ that we used is the bound (5.11). However, this type of bound holds for all positive, integer-valued, multiplicative, prime-independent functions $f(n)$ such that $f(p^\alpha) = g(\alpha)$, $g(\alpha_0) > 1$ for some α_0 and $g(\alpha) < \exp(C\alpha)$ for some $C = C_f > 0$. Repeating the proof of Theorem 7 with obvious modifications we find that there exist at least $x^{1/2}$ numbers from $[x,2x]$ such that all the values $f(n+1)$, $f(n+2),\ldots,$ $\ldots, f(n+t)$ are distinct if $t = [C_1(\log x)^{1/2}/\log\log x]$ with a suitable $C_1 = C_1(f) > 0$. In particular, $d_k(p^\alpha) \ll_k 2^{k\alpha}$, hence this result holds for the function

$d_k(n)$. In the special case $k = 2$ this was already established, by a different method, by P. Erdős and L. Mirsky [5], but for general $d_k(n)$ it appears to be new.

Finally we point out how in the case of $a(n)$ one can obtain that the values $a(n+1),\dots,a(n+t)$ are all distinct for $t = [C(\log x/\log\log x)^{1/2}]$. For this it suffices to note that, analogously to the discussion made in proving Theorem 6, we may take all the m_i's in (5.8) to be squarefree. In view of $a(m_i) = 1$ this immediately implies (5.10), but now we can take $r = r_0$ and not as large as $[C\log\log x]$, which we had before. Thus now $B \le x^{1/25}$ will be satisfied for $t = [C(\log x/\log\log x)^{1/2}]$ and a suitable $C > 0$, and Theorem 7 follows. This improves the previous t by a factor of $(\log\log x)^{1/2}$.

REFERENCES

[1] CARLITZ, L., On a problem in additive arithmetic II., *Quart. J. Math. Oxford 3* (1932), 273-290.

[2] DELANGE, H., Sur des formules de Atle Selberg, *Acta Arith.* 19 (1971), 115-146.

[3] ERDŐS, P. Some asymptotic formulas for multiplicative functions, *Bull. Amer. Math. Soc.* 53 (1947), 536-544.

[4] ERDŐS, P. and SZEKERES, G., Über die Anzahl Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem, *Acta Scien. Math. Szeged* 7 (1935), 95-102.

[5] ERDŐS, P. and MIRSKY, L., The distribution of the values of the divisor function d(n), *Proc. London Math. Soc.* (3) 2 (1952), 257-271.

[6] ERDŐS, P., POMERANCE C. and SÁRKÖZY, A., On locally repeated values of certain arithmetic functions III, *Proc. Amer. Math. Soc.* 101(1987),1-7.

[7] FRIEDLANDER, J.B. and IWANIEC, H., Incomplete Kloosterman sums and a divisor problem, *Ann. Math. II.* Ser. 121 (1985), 319-350.

[8] HALL, R.R., Squarefree numbers in short intervals, *Mathematika 29* (1982), 7-17.

[9] HEATH-BROWN, D.R., The fourth power moment of the Riemann zeta-function, *Proc. London Math. Soc. 38* (1979), 385-422.

[10] HEATH-BROWN, D.R., The square sieve and consecutive square-free numbers, *Math. Ann. 266* (1984), 251-259.

[11] HEATH-BROWN, D.R., The divisor function at consecutive integers, *Mathematica 31* (1984), 141-149.

[12] HERZOG, J., Eine asymptotische Formel für eine Partitionenfunktion von A. Ivić, *Analysis 5* (1985), 185-196.

[13] HERZOG, J. and SCHWARZ, W., Über eine spezielle Partitionenfunktion, die mit der Anzahl der Abelscher Gruppen der Ordnung n zusammenhängt, *Analysis 5* (1985), 153-161.

[14] HILDEBRAND, A., The divisor problem at consecutive integers, *Pacific J. Math.* 129(1987),307-319.

[15] IVIĆ, A., On the number of Abelian groups of a given order and on certain related multiplicative functions, *J. Number Theory 16* (1983), 119-137.

[16] IVIĆ, A. and TENENBAUM, G., Local densities over integers free of large prime factors, *Quart. J. Math.* Oxford (2) 37 (1986), 401-417.

[17] KOLESNIK, G., On the number of Abelian groups of a given order, *J. Reine Angew. Math.* 329 (1981), 164-175.

[18] KNOPP, M.I., Modular functions in analytic number theory, Markham, Chicago, 1970.

[19] KRÄTZEL, E., Die maximale Ordnung der Anzahl der wesentlich verschiedenen Abelscher Gruppen n-ter Ordnung, *Quart. J. Math. Oxford* (2) 21 (1970), 273-275.

[20] KRÄTZEL, E., Die Werteverteilung der nicht-isomorphen Abelschen Gruppen endlicher Ordnung und ein verwandtes zahlentheoretisches Problem, Publs. Inst. Math. Belgrade 31 (45) (1982), 93-101.

[21] MIRSKY, L., Note on an asymptotic formula connected with r-free integers, *Quart. J. Math. Oxford* 18 (1947), 178-182.

[22] MIRSKY, L., On the frequency of pairs of square-free numbers with a given difference, *Bull. Amer. Math. Soc.* 55 (1949), 936-939.

[23] MIRSKY, L., Arithmetical pattern problems relating to divisibility by r-th powers, *Proc. London Math. Soc.* (2) 50 (1949), 497-508.

[24] MIRSKY, L., Summation formulae involving arithmetic functions, *Duke Math. J.* 16 (1949), 261-272.

[25] NAIR, M. and SHIU, P., On some results of Erdős and Mirsky, *J. London Math. Soc.* (2) 22 (1980), 197-203.

[26] NICOLAS, J.-L., Sur les entiers N pour lesquels il y a beaucoup de groupes abéliens d'ordre N, *Ann. Inst. Fourier* (Grenoble) 28 (1978), 1-16.

[27] NICOLAS, J.-L., Sur la distribution des nombres ayant une quantité fixée de facteurs premiers, *Acta Arith.* 44 (1984), 191-200.

[28] SCHWARZ, W. and WIRSING, E., The maximal order of non-isomorphic Abelian groups of order n, *Arch. Math.* 24 (1973), 59-62.

[29] SHIU, P., Note on a result of Erdős and Mirsky, *J. London Math. Soc.* (2) 17 (1978), 228-230.

[30] TIJDEMAN, R., On integers with many small prime factors, *Compositio Math.* 26 (1973), 319-330.

ERDÖS, P.
Matematikai Kutató Intézet
Reáltanoda utca 13-15.
H-1053. Budapest, V.
Hungary

IVIĆ, A.
Katedra Matematike
RGF-a Universiteta u Beogradu
Djušina 7, 11000 Beograd
Yugoslavia

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON SOME PROBLEMS OF THE STATISTICAL THEORY OF PARTITIONS

ERDŐS P. and SZALAY M.*

INTRODUCTION

In what follows we are dealing with partition problems, partly motivated by the statistical theory of groups.

Let Π be a generic "unrestricted" partition of the positive integer n, i.e.,

$$(1.1)\qquad \Pi: \begin{array}{ll} \lambda_1+\lambda_2+\ldots+\lambda_m=n, & \lambda_1\geqq\lambda_2\geqq\ldots\geqq\lambda_m\ (\geqq 1), \\ \lambda_j\text{'s integers}, & m=m(\Pi). \end{array}$$

As to the number p(n) of unrestricted partitions of n, according to the theorem of G.H. HARDY and S. RAMANUJAN from 1918 (see [9]), we have

* Research partially supported by Hungarian National Foundation for Scientific Research grant no. 1811.

$$(1.2)\quad p(n) = (1 - c_o n^{-1/2} + O(n^{-1}))\ \frac{1}{4n\sqrt{3}}\ \exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right)$$

with $c_o = \frac{\sqrt{6}}{2\pi} + \frac{\pi}{24\sqrt{6}}$.

It is well-known that the number of conjugacy classes of the symmetric group of degree n is equal to p(n) and the number of conjugacy classes of the alternating group of degree n is asymptotically equal to $\frac{1}{2}p(n)$ (see [4]).

L.B. BEASLEY, J.L. BRENNER and A.G. WILLIAMSON proved that almost all conjugacy classes of the alternating group of degree n contain a pair of generators. Their original proof could be simplified by proving the fact that almost all partitions Π of n (i.e., apart from $o(p(n))$ Π's at most) have a summand which is >1 and is relatively prime to the other summands. This result can be proved in a reasonable way choosing a suitable *prime*-summand (see [1], Theorem 3.04). We should like to point out here only the fact that this choice is *necessary* in the following sense.

THEOREM 1. *For almost all* Π*'s, if* $\lambda_j > 1$ *and* $(\lambda_j, \lambda_i) = 1$ *for each* $i \neq j$ *then* λ_j *is a prime.*

The nontrivial part of the proof (see Section 2) is the investigation of the λ_j's of the form pq where p and

q are prime numbers.

Next, let Π^* be a generic (unrestricted) *unequal* partition of n, i.e.,

$$\alpha_1+\alpha_2+\ldots+\alpha_m=n, \quad \alpha_1>\alpha_2>\ldots>\alpha_m \ (\geq 1),$$

(1.3) Π^*:

$$\alpha_j\text{'s integers}, \quad m=m(\Pi^*).$$

Their number q(n) is

$$\sim \frac{1}{4\, n^{3/4}\, 3^{1/4}} \exp\left(\frac{\pi}{\sqrt{3}}\sqrt{n}\right)$$

(see [9]).

We investigate the maximal number of consecutive summands in almost all unequal partitions of n. If we consider a fixed positive integer then the probability of its appearing in a randomly chosen Π^* is asymptotically equal to 1/2 ($n\to\infty$). Thus, a fixed consecutive k-tuple will appear with probability $\approx 2^{-k}$ only, therefore we have to consider many k-tuples. Let $M(\Pi^*)$ denote the maximal number of consecutive summands in Π^*. We assert the following

THEOREM 2. *Let us suppose that* $\omega(n)\to\infty$ *(arbitrarily slowly). Then, for almost all* Π^**'s (i.e., with the exception of* $o(q(n))$ Π^**'s at most), we have*

$$(1.4) \quad M(\Pi^*) = \frac{1}{2\log 2}\log n - \frac{1}{\log 2}\log\log n + O(\omega(n)).$$

The proof (see Section 3) is based on the following lemma which is interesting in itself too. For arbitrary positive integers n, k and $a_1, a_2, \ldots, a_k$ with $1 \leq a_1 < a_2 < \ldots < a_k \leq n$, let $q(n; \overline{a_1}, \ldots, \overline{a_k})$ denote the number of unequal partitions of n not having summands from $\{a_1, \ldots, a_k\}$.

LEMMA 1. *Let* ε *be fixed,* $0 < \varepsilon < 10^{-2}$. *For*

$$1 \leq k \leq n^{(1/6)-\varepsilon}, \tag{1.5}$$

we have

$$q(n; \overline{a_1}, \ldots, \overline{a_k}) = (1 + o(1)) \frac{q(n)}{\prod_{j=1}^{k} (1+\exp(-\frac{\pi a_j}{2\sqrt{3n}}))}. \tag{1.6}$$

Here the a_j's were arbitrary, only their number was limited. Restricting their sum too, we can easily estimate the number $q(n; a_1, \ldots, a_k)$ of unequal partitions of n, *containing* each a_j as a summand.

LEMMA 2. *Let* ε *be fixed,* $0 < \varepsilon < 10^{-2}$. *For*

$$1 \leq k \leq n^{(1/6)-\varepsilon} \text{ and } a_1 + \ldots + a_k \leq n^{(3/4)-\varepsilon}, \tag{1.7}$$

we have

$$q(n; a_1, \ldots, a_k) = (1+o(1)) \frac{q(n)}{\prod_{j=1}^{k} (1+\exp(+\frac{\pi a_j}{2\sqrt{3n}}))}. \tag{1.8}$$

Taking into account the fact (see [6], Lemma 10) that in almost all unequal partitions of n the maximal summand is $O(\sqrt{n}\log n)$, Lemma 2 yields the upper estimation of $M(\Pi^*)$. The lower estimate can be proved by a probabilistic argument. We can prove without much difficulty that there exists a distribution function f(x) so that the number of Π^*'s with

$$M(\Pi^*) \geq \frac{\log n}{2 \log 2} - \frac{\log\log n}{\log 2} - x$$

is $(f(x) + o(1))\, q(n)$.

Finally, let $T_n(k)$ denote the number of solutions of $x^k = e$ in the symmetric group of degree n (e is the unit element). It is trivial that

$$T_n(k) = \sum_{\substack{m_d \geq 0 \\ \sum_{d|k} d.m_d = n}} \frac{n!}{\prod_{d|k} (m_d!.d^{m_d})}.$$

Here the summation refers to the partitions Π (of n) having only summands dividing k. S. CHOWLA, I.N.HERSTEIN and W.R. SCOTT [3] posed the problem of the asymptotic behaviour of $T_n(k)$, for fixed integer $k \geq 2$, as $n \to \infty$. They found the generating function $\exp(\sum_{d|k} z^d/d)$ for $T_n(k)/n!$. The problem of the asymptotic behaviour of $T_n(k)$ was solved for k=2 by S. CHOWLA, I.N. HERSTEIN

and K. MOORE [2] and for k=p (fixed prime) by L. MOSER and M. WYMAN [10], [11]. A.I. PAVLOV [12] obtained the logarithmic asymptotic formula $T_n(k) = \exp((1 + o(1))(1 - k^{-1})\, n \log n)$ for any fixed $k \geq 2$, as $n \to \infty$. L.M. VOLYNETS [13] proved that the asymptotic relation

$$(1.9) \quad T_n(k) \sim \left(\frac{n}{e}\right)^n n^{-n/k}\, k^{-1/2} \exp\left(\sum_{d|k} \frac{n^{d/k}}{d} - \frac{1+(-1)^k}{4k}\right)$$

holds for any fixed $k \geq 2$, as $n \to \infty$. The same result (in another form) was proved independently by H.S. WILF[15]. The asymptotic result applies without change to the number of elements of order k too.

The above results refer to fixed k's. For k=k(n), the problem of the asymptotic behaviour of $T_n(k)$ is connected with the statistical theory of groups (see [8], pp. 175, 176). The special case k = n was investigated by R. WARLIMONT [14]. He proved that

$$T_n(n) = (1 + (1+(-1)^n)n^{-1} + O(n^{\varepsilon-2}))(n-1)! \sim (n-1)!$$

which exceeds the "corresponding" expression in (1.9).

Our purpose is to extend (1.9) for the case when k depends on n. As a first step, it is easy to prove (1.9) for

$$(1.10) \qquad 1 \leq k \leq \frac{\log n}{2 \log \log n}.$$

From "log n" the situation can change depending on the arithmetic structure of k (and on its connection with

n). Namely, in Section 4 we prove the following estimate.

THEOREM 3. *Let* ε *be fixed,* $0 < \varepsilon < 10^{-2}$. *For*

$$1 \leq k \leq n^{(1/4)-\varepsilon} \quad \textit{and} \quad n \to \infty, \tag{1.11}$$

we have

$$T_n(k) = \{1+o(1)+f(k,n)\}\frac{n!}{n^{n/k}\sqrt{2\pi nk}} \exp\Big(\sum_{d|k} \frac{n^{d/k}}{d} - \frac{1+(-1)^k}{4k}\Big), \tag{1.12}$$

where

$$f(k,n) = 2\,\mathrm{Re}\Big\{\sum_{j=1}^{[(k-1)/2]} \exp\Big(-i\frac{2jn\pi}{k} + \sum_{d|k} \frac{n^{d/k}}{d}\big(\exp\big(i\frac{2jd\pi}{k}\big)-1\big)\Big)\Big\} + (1+(-1)^k)\frac{(-1)^n}{2}\exp\Big(-2\sum_{\substack{d|k\\ 2\nmid d}}{}' \frac{n^{d/k}}{d}\Big).$$

If $k=p$ (prime), $p \geq \log^2 n$ and $p \mid n$ then the new contribution $f(k,n)$ is $\geq ck$. Next, if k has a divisor $d_o \sim \log\log n$ and $k \leq \exp(2^{-1}\log n/\log\log n)$, then the new contribution is only $o(k)$.

2. PROOF OF THEOREM 1.

From (1.2) we obtain that, for $n \geq 2$ and $1 \leq t \leq n^{1/2}$,

$$(2.1)\quad \frac{p(n-t)}{p(n)} = (1+0(n^{-1}))\,(1+\frac{t}{n} - \frac{\pi t^2}{4\sqrt{6}\, n^{3/2}})\exp(-\frac{\pi t}{\sqrt{6n}})$$

and that, for $n \geq 2$ and $1 \leq t \leq n^{5/8}$,

$$(2.2)\quad \frac{p(n-t)}{p(n)} = (1+0(n^{-1/2}))\,(1+\frac{t}{n} - \frac{\pi t^2}{4\sqrt{6}\, n^{3/2}})\exp(-\frac{\pi t}{\sqrt{6n}})\,.$$

For

$$x_n = \frac{n^{1/4}\ \log^{1/2} n}{\log\log n}\,,$$

we get $\sum_{p \leq x_n} p = o(n^{1/2})$. By (2.2), this implies that almost all partitions Π of n contain each prime $p \leq x_n$ as a summand. Taking into account the theorem of P. ERDŐS and J. LEHNER [5], the maximal summand is

$(1 + o(1))\ \frac{\sqrt{6}}{2\pi}\sqrt{n}\log n$ in almost all Π's. Let us suppose that $\lambda_j > 1$ and $(\lambda_j, \lambda_i) = 1$ for each $i \neq j$. The previous remark on the primes $\leq x_n$ shows that, for almost all Π's, λ_j has at most two prime factors.

First, we suppose that $\lambda_j = pq$ where p and q are prime numbers, $p<q$. Obviously, it is enough to investigate the following case.

$$(2.3)\quad \frac{n^{1/4}\ \log^{1/2} n}{\log\log n} < p < q < n^{1/4}\ \log^{1/2} n\ \log\log n.$$

The number $p(n; \bar{p}, \bar{q})$ of Π's containing neither the summand p nor the summand q can be easily estimated by

means of (2.1).

$$\frac{p(n;\ \bar{p},\ \bar{q})}{p(n)} = 1 - \frac{p(n-p)}{p(n)} - \frac{p(n-q)}{p(n)} + \frac{p(n-p-q)}{p(n)} = \frac{\pi^2 pq}{6n} + O(n^{-3/4}\log^3 n).$$

We have to investigate the following sum:

$$\sum_{(2.3)} p(n-pq;\ \bar{p},\ \bar{q})$$

where the summation refers to the primes p and q satisfying (2.3). Using $n-pq=n(1+O(n^{-1/2}\log^2 n))$ and (2.2) we obtain that

$$\sum_{(2.3)} p(n-pq;\ \bar{p},\ \bar{q}) = \sum_{(2.3)} p(n-pq)\left(\frac{\pi^2 pq}{6(n-pq)} + O(n^{-3/4}\log^3 n)\right) =$$

$$= p(n) \sum_{(2.3)} (1 + O(n^{-1/4}\log^4 n))\ \frac{\pi^2 pq}{6n} \exp\left(-\frac{\pi pq}{\sqrt{6n}}\right) =$$

$$= O(n^{-1})p(n)\exp(-\pi 6^{-1/2}\log n(\log\log n)^{-2})$$

$$\left(\sum_{p\le n^{1/4}\log n} p\right)^2 = o(p(n)).$$

Next, we suppose that $\lambda_j = p^2$ where p is a prime number. It is enough to investigate the case

$$(2.4) \qquad \frac{n^{1/4}\log^{1/2} n}{\log\log n} < p < n^{1/4}\log^{1/2} n$$

and we obtain that

$$\sum_{(2.4)} p(n-p^2;\ \bar{p},\ \overline{2p}) = o(p(n)).$$

3. PROOF OF THEOREM 2.

For $1 \leqq k \leqq n^{1/5}$ and $n \to \infty$, we proved that

$$q(n; \overline{1}, \overline{2}, \ldots, \overline{k}) = (1 + o(1))\frac{q(n)}{2^k}$$

(see [7] , pp. 432-440). We prove Lemma 1 in the same way, detailing only the changes. Let us define the function $h(z) = h_{a_1,\ldots,a_k}(z)$ by

$$(3.1)\quad h(z) = \{\prod_{\nu=1}^{\infty} (1+\exp(-\nu z))\} \{\prod_{j=1}^{k} (1+\exp(-a_j z))\}^{-1}$$

for $x = \mathrm{Re}\, z > 0$. Choosing

$$(3.2)\qquad x = x_o = \frac{\pi}{2\sqrt{3n}} ,$$

we have

$$(3.3)\quad q(n; \overline{a_1}, \ldots, \overline{a_k}) = \frac{1}{2\pi} \int_{-\pi}^{\pi} h(x_o+iy)\, \exp(nx_o+iny)\, dy.$$

We choose again

$$(3.4)\quad y_1 = n^{-3/4+\varepsilon/3}, \quad y_2 = C_o x_o$$

with a sufficiently large constant C_o.

For $|y| \leqq y_1$, using (1.5) we get

$$\{\prod_{j=1}^{k} (1 + \exp(-a_j(x_o+iy))\}^{-1} =$$

$$= \{\prod_{j=1}^{k} (1+\exp(-a_j x_o))\}^{-1} \exp\{-\sum_{j=1}^{k} \log(1 - \frac{1-\exp(-ia_j y)}{\exp(a_j x_o)+1})\} =$$

$$= \{ \prod_{j=1}^{k} (1+\exp(-a_j x_o)) \}^{-1} \exp\{0(n^{(1/6)-\varepsilon} y_1/x_o)\},$$

therefore (cf. [7], pp. 435-437),

$$\frac{1}{2\pi} \int_{-y_1}^{y_1} = (1 + o(1))\, q(n) \{ \prod_{j=1}^{k} (1+\exp(-a_j x_o)) \}^{-1}.$$

For $|y| \leq \frac{x_o}{2k}$,

$$\left| \sum_{j=1}^{k} \log \frac{1}{1 - \frac{1 - \exp(-ia_j y)}{\exp(a_j x_o)+1}} \right| \leq \sum_{j=1}^{k} \log \frac{1}{1 - \frac{|1-\exp(-ia_j y)|}{\exp(a_j x_o)+1}} =$$

$$= 0(k\,|y|/x_o) = 0(1).$$

For $\frac{x_o}{2k} \leq |y| \leq \pi$, the above sum can be estimated by

$$\sum_{j=1}^{k} \log \frac{1}{1 - \frac{2}{\exp(a_j x_o)+1}} \leq k \log \frac{1}{1 - \frac{2}{\exp(x_o)+1}} = 0(k \log n),$$

consequently,

$$\frac{1}{2\pi} \int_{x_o/2k}^{y_2} = 0(1) \{ \prod_{j=1}^{k} (1+\exp(-a_j x_o)) \}^{-1} \exp\{ \frac{\pi^2 x_o}{12(x_o^2 + x_o^2 (2k)^{-2})} +$$

$$+ n x_o + 0(k \log n) \}.$$

By (1.5), $k \log n = o(n^{1/2} k^{-2})$ and we can finish the proof as in [7].

Lemma 1 easily yields Lemma 2 since $q(n; a_1,\dots,a_k) = q(n-a_1-\dots-a_k; \overline{a_1}, \dots, \overline{a_k})$ and the restrictions in (1.7) imply that

$$q(n-a_1-\dots-a_k) = (1 + o(1))\, q(n) \prod_{j=1}^{k} \exp\left(-\frac{\pi a_j}{2\sqrt{3n}}\right)$$

and

$$n - a_1 - \dots - a_k = n\,(1 + 0(n^{-(1/4)-\varepsilon})).$$

For almost all Π^*'s, $\alpha_1 \leq \left(\frac{\sqrt{3}}{\pi} + o(1)\right) \sqrt{n} \log n$

(see [6], Lemma 10, p. 206). Therefore, Lemma 2 yields that, for

$k = [\frac{\log n}{2 \log 2} - \frac{\log \log n}{\log 2} + \omega(n)]$, $K = [\sqrt{n} \log n]$, $\omega(n) \to \infty$ and $\omega(n) \leq \log \log n$,

$$\sum_{\Pi^*} 1 \leq o(q(n)) + \sum_{t=0}^{K} q(n; t+1, \dots, t+k) =$$

$M(\Pi^*) \geq k$

$$= o(q(n)) + \sum_{t=0}^{K} (1+o(1)) q(n) \prod_{j=1}^{k} \left(1+\exp\left(\frac{\pi(t+j)}{2\sqrt{3n}}\right)\right)^{-1} =$$

$$= o(q(n)) + (1 + o(1))\, q(n) \sum_{t=0}^{K} \left(1+\exp\left(\frac{\pi t}{2\sqrt{3n}}\right)\right)^{-k} =$$

$$= o(q(n)) + (1 + o(1))\, q(n) \int_0^{\infty} \left(1+\exp\left(\frac{\pi t}{2\sqrt{3n}}\right)\right)^{-k} dt =$$

$$= o(q(n)) + (1 + o(1))\, q(n)\, \frac{2\sqrt{3n}}{\pi} \int_2^{\infty} x^{-k-1} (1-x^{-1})^{-1}\, dx =$$

$$= o(q(n)) + (1 + o(1))\, q(n)\, \frac{4\sqrt{3}}{\pi} \cdot \frac{\sqrt{n}}{k.2^k} = o(q(n)).$$

This proves the upper estimation in Theorem 2.

Now, for

$$k = [\frac{\log n}{2 \log 2} - \frac{\log \log n}{\log 2} - \omega(n)],\ K = [\sqrt{n} \log n],\ \omega(n) \to \infty \text{ and}$$

$$\omega(n) \leqq \log \log n,$$

let $f(\Pi^*, k)$ denote the number of t's from $[0,K]$ with the property that Π^* contains $t+1, \ldots, t+k$ as summands. Then we obtain that

$$E \doteq \frac{1}{q(n)} \sum_{\Pi^*} f(\Pi^*,k) = \frac{1}{q(n)} \sum_{t=0}^{K} q(n;\ t+1, \ldots, t+k) =$$

$$= (1 + o(1))\ \frac{4\sqrt{3}}{\pi} \cdot \frac{\sqrt{n}}{k.2^k},$$

$$E^{-1} = o(1),$$

$$\frac{1}{q(n)} \sum_{\Pi^*} f^2(\Pi^*,k) \leqq 0(E)(1 + \frac{1}{2} + \ldots + \frac{1}{2^k}) + (1 + o(1))\, E^2,$$

$$\frac{1}{q(n)} \sum_{\Pi^*} (f(\Pi^*,k) - E)^2 \leqq 0(E) + o(E^2) = o(E^2).$$

Therefore,

$$\sum_{\substack{\Pi^* \\ f(\Pi^*,k)=0}} 1 = o(q(n))$$

and we get the lower estimation in Theorem 2.

4. PROOF OF THEOREM 3.

Let us observe that

$$\sum_{n=0}^{\infty} \frac{T_n(k)}{n!} z^n = \exp\Big(\sum_{d|k} \frac{z^d}{d} \Big)$$

for arbitrary complex z's. With the *explicit* radius

$$R = n^{1/k} , \tag{4.1}$$

Cauchy's formula gives the representation

$$T_n(k) = \frac{n!}{n^{n/k}} \exp\Big(\sum_{d|k} \frac{n^{d/k}}{d} \Big) \frac{1}{2\pi} \int_{-\pi}^{\pi} \exp\Big\{ \sum_{d|k} \frac{n^{d/k}}{d} (\cos(d\phi) - 1) +$$

$$+ i \Big(\sum_{d|k} \frac{n^{d/k}}{d} \sin(d\phi) - n\phi \Big) \Big\} d\phi .$$

Let $c_1 = \frac{1}{2} - \frac{\varepsilon}{2}$ and

$$\delta = \begin{cases} 1 & \text{if } 2|k \\ 0 & \text{if } 2 \nmid k . \end{cases}$$

Then we get from (1.11)

$$n^{-c_1} \int_{-n^{-c_1}}^{n^{-c_1}} \exp\Big\{ -\frac{1}{2} \Big(\sum_{d|k} n^{d/k} . d \Big) \phi^2 + \delta i\, n^{1/2} \phi +$$

$$+ O(n^{-c_1 + \frac{1}{3}}) (1 + k^2 n^{-2c_1 + \frac{2}{3}}) \Big\} d\phi =$$

$$= \frac{\sqrt{2\pi}}{\Big(\sum_{d|k} n^{d/k} . d \Big)^{1/2}} \exp\Big(-\frac{\delta}{2k} \Big) (1 + o(1)) = \frac{\sqrt{2\pi}}{\sqrt{nk}} \exp\Big(-\frac{\delta}{2k} \Big) (1 + o(1)).$$

For $n^{-c_1} \leq |\phi| \leq \frac{\pi}{k}$, we can get trivial estimations from d=k, resulting $o((nk)^{-1/2})$.

For $\frac{\pi}{k} \leq |\phi| \leq \pi$, we can estimate by

$$2 \sum_{j=1}^{[k/2]} \int_{(2j-1)\pi/k}^{(2j+1)\pi/k} \exp\{n^{1/k}(\cos\phi - 1) + \frac{n}{k}(\cos(k\phi) - 1)\} d\phi =$$

$$= O(\exp(-2\, n^{1/k} k^{-2} + \log k))(nk)^{-1/2}.$$

These imply (1.9) for $1 \leq k \leq \log n\ (2 \log\log n)^{-1}$.

Now, let

$$\frac{\log n}{2 \log\log n} \leq k \leq n^{(1/4)-\varepsilon} \tag{4.2}$$

and a similar division gives (for $\frac{\pi}{k} \leq |\phi| \leq \pi$)

$$o((nk)^{-1/2}) + 2\mathrm{Re}\left\{ \sum_{j=1}^{[(k-1)/2]} \int_{-\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}}^{\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}} \exp\left\{ \sum_{d|k} \frac{n^{d/k}}{d} (\cos(d\phi + \frac{2jd\pi}{k}) - 1) + i\left(\sum_{d|k} \frac{n^{d/k}}{d} \sin(d\phi + \frac{2jd\pi}{k}) - n\phi - \frac{2jn\pi}{k} \right) \right\} d\phi + \right.$$

$$\left. + \delta \cdot \int_{-\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}}^{0} \exp\{\ldots\} d\phi \right\} = o((nk)^{-1/2}) + 2\ \mathrm{Re}\left\{ \sum_{j=1}^{[(k-1)/2]} \exp \right.$$

$$\left. \left\{ - i\, \frac{2jn\pi}{k} + \sum_{d|k} \frac{n^{d/k}}{d} (\exp(i\frac{2jd\pi}{k}) - 1) \right\} \right.$$

$$\left. \cdot \int_{-\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}}^{\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}} \exp\{ \frac{n}{k}(e^{ik\phi} - 1 - ik\phi) + \frac{2\delta n^{1/2}}{k}(-1)^j\, i\, \frac{k}{2}\phi \} d\phi + \right.$$

$$+\delta.\exp\{-\ in\ \pi+$$

$$+\sum_{d|k}\frac{n^{d/k}}{d}(e^{id\pi}-1)\}\int_{-\frac{\pi\sqrt{\log k}}{\sqrt{2nk}}}^{0}\exp\{\frac{n}{k}(e^{ik\phi}-1-ik\phi)\}d\phi\Bigg\}$$

and one can obtain (1.12) by routine calculations.

REFERENCES

1 L.B. BEASLEY, J.L. BRENNER, P. ERDŐS, M. SZALAY and A.G. WILLIAMSON, Generation of alternating groups by pairs of conjugates, *Periodica Math. Hung.* 18 (1987), 259-269.

2 S. CHOWLA, I.N. HERSTEIN and K. MOORE, On recursions connected with symmetric groups, I, *Canad. J. Math.* 3 (1951), 328-334.

3 S. CHOWLA, I.N. HERSTEIN and W.R. SCOTT, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk.* 25 (1952), 29-31.

4 J. DÉNES, P. ERDŐS and P. TURÁN, On some statistical properties of the alternating group of degree n, *L'Enseignement mathématique* XV (1969), 89-99.

5 P. ERDŐS and J. LEHNER, The distribution of the number of summands in the partitions of a positive integer, *Duke Math. Journal* 8 (1941), 335-345.

6 P. ERDŐS and M. SZALAY, On some problems of J. DÉNES and P. TURÁN; in: Studies in Pure Mathematics (To the Memory of Paul Turán), *Akadémiai Kiadó*, Budapest, 1983, 187-212.

7 P. ERDŐS and M. SZALAY, On the statistical theory of partitions; in: Colloquia Math. Soc. J. Bolyai 34. *Topics in Classical Number Theory* (Budapest, 1981), 397-450, North-Holland/Elsevier.

8 P. ERDŐS and P. TURÁN, On some problems of a statistical group theory, I, *Z. Wahrscheinlichkeitstheorie und verw. Gebiete* 4 (1965), 175-186.

9 G.H. HARDY and S. RAMANUJAN, Asymptotic formulae in combinatory analysis, *Proc. of the London Math. Soc.* (2) XVII (1918), 75-115.

10 L. MOSER and M. WYMAN, On the solutions of $x^d = 1$ in symmetric groups, *Canad. J. Math.* 7(1955), 159-168.

11 L. MOSER and M. WYMAN, Asymptotic expansions, *Canad. J. Math.* 8(1956), 225-233.

12 A.I. PAVLOV, On the number of solutions of the equation $x^k = a$ in the symmetric group (in Russian), *Mat. Sb.* 112(1980), 380-395.

13 L.M. VOLYNETS, On the number of solutions of the equation $x^s = e$ in the symmetric group (in Russian), *Mat. Zametki* 40 (1986), 155-160. {English translation: *Math. Notes* 40(1986), 586-589.}

14 R. WARLIMONT, Über die Anzahl der Lösungen von $x^n=1$ in der symmetrischen Gruppe S_n, *Arch.Math.*30(1978), 591-594.

15 H.S. WILF, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc.* 15(1986), 228-232.

Note added in proof. L.M. Volynets [The number of solutions of an equation in the symmetric group (in Russian); in: *Probabilistic processes and their applications*, Interuniv. Collect., Moscow, 1985, pp.104-109] determined the asymptotic behaviour of $T_n(p)$ for any *prime* p depending on n.

ERDÖS, P.

Mathematical Institute of the Hungarian Academy of Sciences
H-1053 Budapest, Reáltanoda u. 13-15. H u n g a r y

SZALAY, M.

Department of Algebra and Number Theory
Eötvös Loránd University
H-1088 Budapest, Muzeum körut 6-8. H u n g a r y

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON REAL-VALUED R-ADDITIVE FUNCTIONS

FEHÉR J.

1. INTRODUCTION

Let $q \geq 2$ be a fixed integer. Any positive integer n can uniquely be represented in the form $n=a_0 a_1 q + \ldots + a_s q^s$ $(0 \leq a_i < q)$. We call a function $f: \mathbb{N}_0 \to C$ q-additive if $f(0)=0$ and $f(n)=f(a_0) + f(a_1 q) + \ldots + f(a_s q^s)$.

DEFINITION 1. Let R_i be a subset of $\mathbb{N}_0$ $(i=0,1,\ldots)$. The family $R = \{R_0, R_1, \ldots\}$ is an R-system, if the following conditions are satisfied:

(a) $0 \in R_i$, $1 < |R_i| \leq \infty$ $(i=0,1,\ldots)$;

(b) the smallest positive element of R_i is smaller than the smallest positive element of R_j, whenever $0 \leq i < j$;

(c) any positive integer n can uniquely be represented

in the form

(1.1) $n = r_o + r_1 + \ldots + r_s$ $(r_i \in R_i,\ s \geq 1)$.

DEFINITION 2. The function $f : \mathbb{N}_o \to C$ is called R-additive (with respect to a given R-system) if $f(0) = 0$ and $f(n) = f(r_o) + f(r_1) + \ldots + f(r_s)$, whenever n has the form (1.1).

The notion of q-additivity is due to A.O. GELFOND ([3]), R-additivity was introduced in [1]. Here we deal with real-valued R-additive functions only. A(R) denotes (for a given R-system) the space of all real-valued R-additive functions.

In part 2 let the R-system be arbitrarily fixed. From part 3 on let us consider the special choice $R_o = \{0,1,\ldots,d-1\}$ with $d \geq 2$.

Let for all real α

$$||\alpha|| := \min\{|\alpha - z| : z \in \mathbb{Z}\}.$$

Further let $f_k, f_{k-1}, \ldots, f_1, f_o \in A(R)$ and

$$G(n) := f_k(n+k) + f_{k-1}(n+k-1) + \ldots + f_1(n+1) + f_o(n),$$

and for all $\varepsilon > 0$

$$\delta(\varepsilon) := \liminf_{x \to \infty} \frac{1}{x} \#\{n \mid n \leq x,\ ||G(n)|| \geq \varepsilon\}.$$

THEOREM 1. If $\delta(\varepsilon_o) = 0$, then

(1.2) $||G(n)|| \leq 3\varepsilon_o$ (for all $n \in \mathbb{N}_o$).

COROLLARY. If $\delta(\varepsilon)=0$ for all $\varepsilon>0$, then

(1.3) $\quad G(n)\equiv 0 \pmod 1$ (for all $n\in\mathbb{N}_0$).

In part 2 we prove Theorem 1. The other theorems of the paper consern with the solvability of (1.3) in general, resp., with further restrictions.

2. PROOF OF THEOREM 1.

For a given $R = \{R_0,R_1,\ldots\}$ let

$A_i := \{r_0+r_1+\ldots+r_{i-1} \mid r_j\in R_j\}$ $(i>0)$ and $A_0 := \{0\}$;

$T_i :=$ the set of all numbers, for which we have in (1.1) $r_0=r_1=\ldots=r_{i-1}=0$.

(For example, if $R_0=\{0,1,\ldots,d-1\}$, then $A_1=R_0$ and $T_1=\{Nd \mid N=0,1,\ldots\}$.)

LEMMA. Let $i\geq 0$ and $\alpha\in A_i$ be fixed. Further let $B_i(\alpha, x) := \{n \mid n+\alpha\leq x,\ n\in T_i\}$. Then we have

$$|B_i(\alpha, x)| \sim x/|A_i| \quad (x\to\infty).$$

(Proof of the Lemma see in [2]).

PROOF. Let the index i and $\alpha\in A_i$ be fixed. We introduce the notations

$$H_i(\varepsilon,\alpha, x) := \{n \mid n+\alpha\leq x,\ n\subseteq T_i,\ \|G(n+\alpha)\|\geq\varepsilon\},$$

$$L(n) := f_k(n) + f_{k-1}(n) +\ldots+ f_1(n) + f_0(n),$$

$$D_i(\varepsilon,\alpha, x) := \{n \mid n+\alpha\leq x,\ n\in T_i, \|L(n)\|<\varepsilon\},$$

$M_i(\varepsilon,\alpha,x) := \{n \mid n + \alpha \leq x,\ n \in T_i,\ ||L(n)|| \geq \varepsilon\}$.

By assumption there exists a sequence $x_s \to \infty$, for which

$$(2.1) \qquad \frac{|H_o(\varepsilon_o,0,x_s)|}{x_s} \to 0 \qquad (x_s \to \infty).$$

The relation $|H_i(\varepsilon,\alpha,x) \leq |H_o(\varepsilon_o,0,x)|$ is obviously valid for all $i \geq 0$, $\alpha \in A_i$ and $\varepsilon \geq \varepsilon_o$, hence by (2.1) we have

$$(2.2) \qquad \frac{|H_i(\varepsilon,\alpha,x_s)|}{x_s} \to 0 \quad (i \geq 0,\ \alpha \in A_i,\ \varepsilon \geq \varepsilon_o).$$

By assumption there exists a natural number α with $||G(\alpha)|| < \varepsilon_o$.

We suppose on the contrary, that there exists $\beta \in \mathbf{N}_o$ with $||G(\beta)|| > 3\varepsilon_o$. Let the index i be fixed such that $\alpha, \alpha+1, \ldots, \alpha+k, \beta, \alpha+1, \ldots, \beta+k \in A_i$.

If $n \in M_i(2\varepsilon_o,\alpha,x)$, then $||G(n+\alpha)|| =$

$$= ||L(n) + G(\alpha)|| \geq \varepsilon_o,$$

and hence $M_i(2\varepsilon_o,\alpha,x) \subset H_i(\varepsilon_o,\alpha,x)$. This implies by (2.2)

$$(2.3) \qquad \frac{|M_i(\varepsilon_o,\alpha,x_s)|}{x_s} \to 0 \quad (x_s \to \infty).$$

The relation $||M_i(2\varepsilon_o,\alpha,x)| - |M_i(2\varepsilon_o,\beta,x)|| \leq |\alpha-\beta|$ holds obviously, and hence by (2.3) we infer

$$(2.4) \qquad \frac{|M_i(2\varepsilon_o, \beta, x_s)|}{x_s} \to 0 \quad (x_s \to \infty).$$

As $D_i(2\varepsilon_o, \beta, x) U M_i(2\varepsilon_o, \beta, x) = B_i(\beta, x)$, we have from (2.4) by Lemma

$$(2.5) \qquad \frac{|D_i(2\varepsilon_o, \beta, x_s)|}{x_s} \to 1/|A_1| \quad (x_s \to \infty).$$

Now let $n \in D_i(2\varepsilon_o, \beta, x)$. Then we have $||G(n+\beta)|| = ||L(n) + G(P)|| \geq \varepsilon_o$ and hence $D_i(2\varepsilon_o, \beta, x) \subset H_i(\varepsilon_o, \beta, x)$, which contradicts (2.2), by (2.5). This completes the proof of Theorem 1. □

3. ON THE SOLUTIONS OF (1.3)

THEOREM 2. Let $R_o = \{0, 1, \ldots, d-1\}$ with $d \geq 2$ and $k \geq d$. Then the system $f_k, f_{k-1}, \ldots, f_o \in A(R)$ is a solution of (1.3) if and only if the following conditions hold:

(a) $f_i(Nd) \equiv c_i N \pmod 1$ (for all $N \in \mathbb{N}_o$, $i = 0, 1, \ldots k$);

(b) $c_k + c_{k-1} + \ldots + c_1 + c_o \equiv 0 \pmod 1$;

(c) $G(r) \equiv 0 \pmod 1$ (for all $r \in R_o$),

where $c_k, \ldots, c_o$ are real numbers.

PROOF. It is easy to see that

$$(3.1) \qquad G(Nd+r) = L(Nd) + G(r) \quad (r = 0, 1, \ldots, d-k-1),$$

$$(3.2)\quad \begin{cases} G(Nd+d-j) = \sum_{i=j}^{k} [f_i((N+1)d)-f_i(Nd)-f_i(d)]+ \\ \qquad\qquad +L(Nd)+G(d-j) \\ \text{for all } N\in\mathbb{N}_o,\ j=1,2,\ldots,k). \end{cases}$$

(1) (Necessity) With r=0 (3.1) implies

$$(3.3)\quad L(Nd)\equiv 0 \pmod 1 \quad \text{(for all } N\in\mathbb{N}_o).$$

With j=k we have from (3.2) and (3.3)

$$(3.4)\quad f_k((N+1)d)\equiv f_k(Nd) + f_k(d) \pmod 1$$

i.e.

$$(3.5)\quad f_k(Nd) \equiv Nf_k(d) \pmod 1 \quad \text{(for all } N\in\mathbb{N}_o).$$

This means the necessity of (a) for i=k. Comparing (3.4), (3.3) and (3.2) (with j=k-1) we obtain the necessity of (a) for i=k-1. Hence we get step by step the necessity of (a).

With the choice N=1 (3.3) gives the necessity of (b), while the necessity of (c) is obvious.

(2) (Sufficiency) Now let $(f_k,..,f_o)$ be a system, satisfying (a),(b),(c) ($f_i\in A(R)$). Then we have directly from (3.1) and (3.2) for $n=Nd+r$ $(0\le r<d)$

$$G(n)\equiv (c_k+\ldots+c_1+c_o)N+G(r)\equiv G(r)\equiv 0 \pmod 1. \square$$

4. ON THE SOLUTIONS OF A SPECIAL CASE OF (1.3)

Let $P(z)=a_k z^k+\ldots+a_1 z+a_o \in \mathbb{R}[z]$ $(a_k \neq 0,\ k \geq 1)$, $f \in A(R)$ and $P(E)f(n) := a_k f(n+k)+\ldots+a_a f(n+1) + a_o f(n)$. Then

(4.1) $\quad P(E)f(n) \equiv 0 \pmod 1 \quad$ (for all $n \in \mathbb{N}_o$)

is a special case of (1.3). We may assume that $a_k=1$. Let $R_o=\{0,1,\ldots,d-1\}$.

DEFINITION 3. The function $f \in A(R)$ is called "of type A" whenever $f(Nd)= cN$ (for all $N \in \mathbb{N}_o$) and $P(E)f(r) \equiv 0 \pmod 1$ (for all $r \in R_o$), where c is a real number with $cP(1) \in \mathbb{Z}$.

DEFINITION 4. The function $g \in A(R)$ is called "of type B", if $g(d)=g(d-1)=\ldots=g(1)=g(0)=0$.

The following theorem characterises the R-additive solutions of (4.1).

THEOREM 3. Let $R_o=\{0,1,\ldots,d-1\}$ $(d>1)$ and let $P(z) \in \mathbb{R}[z]$ be a given polynomial with leading coefficient 1, such that $0<\deg P=k<d$. Then any f of type A is a solution of (4.1). Further

(a) if $P(z) \notin Q[z]$, then (4.1) has no other solutions,

(b) if $P(z) \in Q[z]$ and $a_j=p_j/q_j \in \mathbb{Z}$, $(p_j,q_j)=1$, $j=0,\ldots,k)$, then a function g of type B is a solution of (4.1)

if and only if $g(\mathbb{N}_0) \subset \mathbb{Z}$ and $q \mid g(n)$ (for all $n \in \mathbb{N}_0$), where q is the least common multiple of the numbers $q_k, q_{k-1}, \ldots, q_0$.

(c) any solution F of (4.1) can be represented in the form $F=f+g$, where f is a solution of type A and g is a solution of type B.

PROOF. By Theorem 2 any f of type A is a solution of (4.1), (a) Conversely, let $f \in A(R)$ be a solution of (4.1). Then by Theorem 2 we have

(4.2) $a_j f(Nd) \equiv a_j f(d) N \pmod 1$ (for all $N \in \mathbb{N}_0, j=0,1,\ldots,k$).

If $f(d)=c=0$, then f is of type A. Suppose, that $f(d)=c \neq 0$. By $a_k=1$ (4.2) implies $f(Nd) \equiv Nf(d) \pmod 1$. Let some a_j $(0 \leq j \leq k)$ be irrational. Then (4.2) implies $f(Nd)=Nf(d)=cN$, (4.1) for $n=d$ yields which means that f is of type A.

(b) Now let $P(z) \in \mathbb{Q}[z]$ and let g be a solution of type B of (4.1). Then by $g(Nd) \equiv Ng(d) \pmod 1$ and by $g(d) = 0$ we have $g(Nd) \in \mathbb{Z}$. By R-additivity we have $g(\mathbb{N}_0) \subset \mathbb{Z}$. By the conditions $(p_j/q_j)g(Nd) \equiv N(p_j/q_j)g(d)=0 \pmod 1$ and using that $(p_j, q_j)=1$ we obtain $q_j \mid g(Nd)$ (for all $N \in \mathbb{N}_0$). This means $q \mid g(Nd)$ (for all $N \in \mathbb{N}_0$). So for $n=Nd+r$ $(0 \leq r < d)$ we have $g(n) = g(Nd)+g(r)=g(Nd)$, that is $q \mid g(n)$ (for all $n \in \mathbb{N}_0$).

For the converse we see, that any function g of

type B satisfying the conditions is a solution of (4.1). (c) The function g=0 is obviously an R-additive solution of type B of (4.1), hence $P(z) \notin Q[z]$ implies that the statement is true.

Let now $P(z) \subset Q[z]$ and let F be a solution of (4.1). Then $F(Nd)-NF(d) \equiv 0 \pmod{q}$ holds (for all $N \in \mathbb{N}_o$). Let $g(R_o) := \{0\}$ and $g(Nd) := F(Nd)-NF(d)$ with $g \in A(R)$. Then g is a solution of type B of (4.1). As F and g are solutions of (4.1), the same holds for f=F-g. By the definition of g we get that f is of type A. □

5. ON THE SOLUTIONS OF TYPE A OF (4.1)

By Theorem 3 it is eough to determine all solutions of type A. We can reduce this problem as follows.

Suppose, that F is a solution of type A under the assumptions of Theorem 3, that is

$F(Nd)=cN$, $cP(1) \in \mathbb{Z}$ and $P(E)F(r) \equiv 0 \pmod{1}$ (for all $r \in R_o$).

Let $f(n) := dF(n) - cn$. As the function cn is R-additive, f is a real-valued R-additive function with $f(Nd)=0$ (for all $N \in \mathbb{N}_o$) and $P(E)f(n) \equiv -cP'(1) \pmod{1}$ (for all $n \in \mathbb{N}_o$). (Here $P'(z)$ denotes the derivate of $P(z)$). Instead of (4.1) we consider

$$(5.1) \quad \begin{cases} P(E)f(n) \equiv -cP'(1) \pmod{1} \text{ (for all } n \in \mathbb{N}_o) \\ cP(1) \in \mathbb{Z}. \end{cases}$$

In this paper let us call an R-additive solution of (5.1) a principal solution, if $f(Nd) = 0$ (for all $N \in \mathbb{N}_o$) holds.

It is clear, that for any solution F of type A of (4.1) there exists a principal solution of (5.1). Conversely: If f is a principal solution, then the function $F(n)=f(n) + cn$ is of type A. (By Theorem 3, F is a solution of (4.1).)

Our aim is to study the principal solutions.

From now on we use the following notations and assumptions:

$m=d-1$, $R_o=\{0,1,\ldots, m\}$, $P(z)=a_m z^m + \ldots + a_1 z + a_o$. (For deg $P=k<m$ let $a_j=0$ for $j>k$.) Further let $cP(1) \in \mathbb{Z}$. We introduce the notation $f(r)=y_r$ $(r=0,1,\ldots,m)$.

It is clear, that f is a principal solution if and only if $(y_m, y_{m-1}, \ldots, y_1, y_o)$ is a solution of the system

$$
\begin{aligned}
& a_m y_m + a_{m-1} y_{m-1} + \ldots + a_1 y_1 + a_o y_o = B_o \\
& a_{m-1} y_m + a_{m-2} y_{m-1} + \ldots + a_o y_1 + a_m y_o = B_1 \\
& \qquad\qquad \vdots \\
& a_o y_m + a_m y_{m-1} + \ldots + a_2 y_1 + a_1 y_o = B_m
\end{aligned}
\tag{5.2}
$$

Where $y_o=0$. Here B_i is any real number for which $B_i \equiv -cP'(1) \pmod 1$ $(i=0,1,\ldots,m)$.

Let S denote the matrix of the equation-system (5.2) and ρ its rank.

A.) Let $\rho=d$ and $P(z)\in Q[z]$.

By $P(1)\neq 0$ all numbers c with $cP(1)\in \mathbb{Z}$ are rational, hence $cP'(1)$ is rational too. If $cP'(1)\in \mathbb{Z}$, then (5.1) has infinitely many principal solutions.

For case $cP'(1)\notin\mathbb{Z}$ we have proved only

THEOREM 4. For any $m\geq 1$ there exit $P(z)\in Q[z]$ with deg $P=m$, $\rho=d$ and a number c, such that the conditions of Theorm 3 are satisfied but (5.1) has no principal solution.

PROOF. Let us choose the triplets (m,P,c) for example as follows:

1. $m=1$, $P(z)=\frac{3}{2}z+\frac{5}{2}$, $c=\frac{3}{4}$

2. m 2 even, $P(z)=z^m+\frac{}{2m}(z^{m-1}+\ldots+z+1)$, $c=2$

3. $m=2q-1$ $(q>2)$, $P(z)=z^m+\frac{1}{q}(z^{m-1}+\ldots+z)-\frac{q-2}{q}$, $c=1$

4. $m=3$, $P(z)=z^3+\frac{8}{7}$ and $c=\frac{7}{5}$.

Checking the cases is left to the reader. □

B.) Let $\rho=d$ and $P(z)$ has exactly one irrational coefficient. It is clear that (5.1) has a principal solution if and only if

$$(5.3)\qquad D=\begin{vmatrix} a_m & a_{m-1} & \cdots & a_1 & B_o \\ a_{m-1} & a_{m-2} & \cdots & a_o & B_1 \\ & & \vdots & & \\ a_o & a_m & \cdots & a_2 & B_m \end{vmatrix}=0$$

holds with B_i's not all 0. Let $=a_j$ denote the only irrational coefficient. Let us write z for a_j in D, then we obtain the polynomial D(z). Then $D(z) \in Q[z]$ and deg $D \leq m$.

If $cP'(1) \in$, then $B_i=0$ give the trivial solution f=0, which we would like to exclude.

THEOREM 5. Under the conditions of B) let $cP'(1) \in \mathbb{Z}$. Then (5.1) has a principal solution $f \neq 0$ if and only if the following conditions hold:

(a) D(z)=0 (identically) holds for some B_i's such that $B_i \neq 0$ for all i,

(b) θ is an algebraic number of degree at most m over the rational field. □

PROOF is left to the reader.

C) The case $\rho < d$.

THEOREM 6. Let $R_o=\{0,1,\ldots,d-1\}$, further let $P \in \mathbb{R}[z]$, deg $P<d$ and $\rho<d$.

(a) If $P(1) \neq 0$, then (5.1) has a principal solution $f \neq 0$ for any real c which satisfies $cP(1) \in \mathbb{Z}$.

(b) If P(1)=0 and (5.1) has a principal solution $f \neq 0$, then $dcP'(1) \in \mathbb{Z}$.

PROOF.

a) Using the condition $\rho<d$ there exists $\alpha_o,\alpha_1,\ldots,\alpha_m$ not all 0 such that the linear combination of them

with the elements of an arbitrary column of S gives 0. Adding these equations we get

$$(\sum_{i=0}^{m} \alpha_i)P(1)=0$$

Hence $P(1)\neq 0$ yields $\sum_{i=0}^{m} \alpha_i=0$. This implies that det D=0 too for example by the choise $B_i = -cP'(1)$.

b) $P(1) = 0$ implies $\rho<d$. (If we add the first m rows to the last one, we see that det S=0. Let y_i^* denote the solutions of (5.2). Adding the rows of (5.2), we get

$$0=P(1)\sum_{i=0}^{m} y_i^* = \sum_{i=0}^{m} B_i \equiv -cdP'(1) \pmod 1. \square$$

REMARK. If z=0 is a zero of P(z) with multiplicity at least 2, then (5.1) has a principal solution for any real c.

ANCKNOWLEDGEMENT.

The author wants to express his gratitude to Katalin Kovács for his valuable help in the present work especially for the essential simplification of the proof of Theorem 6.

REFERENCES

[1] FEHÉR, J., On a generalization of q-additive functions, *Annales Univ. Sci.* Budapest Sec. Math., 27 (1984) 257-262.

[2] FEHÉR, J., Bemerkungen über R-additive Funktionen, *Annales Univ. Sci.* Budapest Sec. Math. XXIX (1986) 273-281.

[3] GELFOND, A.O., Sur les nomberes qui ont des proprietés additives et multiplicatives données, *Acta Arithm.* 13(1986) 259-265.

J. FEHÉR

Janus Pannonius University
Pécs
Ifjuság u. 6. H-7624

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

A LOWER ESTIMATION FOR THE CARDINALITY OF FINITE DIFFERENCE SETS IN R^n

G. FREIMAN, A. HEPPES and B. UHRIN

1. INTRODUCTION

In what follows the sets A, B are finite subsets of R^n or more specifically of $\Lambda \subset R^n$, where Λ is a point lattice i.e. integer combination of n independent vectors (expecially $\Lambda = Z^n$, the integer vectors). The cardinality of A is denoted by $|A|$ and $-A$ means the set $\{-a: a \in A\}$. We denote by $A+B$ the algebraic sum of the sets. The set $A+A$ is called the sum-set of A and $A-A = A+(-A)$ is the difference set of A.

It is clear that

$$(1.1) \qquad \frac{|A|(|A|+1)}{2} \geq |A+A| \geq 2|A|-1$$

and

(1.2) $|A|^2 - |A| + 1 \geq |A - A| \geq 2|A| - 1$

for any finite $A \subset R^n$.

The structure of sum-sets of $A \subset Z^n$ such that

(1.3) $|A + A| < \text{const}|A|$

(the sum-sets of small cardinality), has been investigated in [1].

On the other hand, little is known about $|A - A|$. A plausible idea is to compare $|A - A|$ with $|A + A|$ and to apply the results for $|A + A|$ (say from [1]).

For example, P. Erdős asked the following question (see [2]):

Is it true that for every constant c there exists another constant c′ such that for any finite $A \subset Z^1$

(1.4) $\frac{|A + A|}{|A|} \leq c$ implies $\frac{|A - A|}{|A|} \leq c'$?

J. Conway conjectured that $|A + A| \leq |A - A|$ for every finite $A \subset Z^1$ but this proved to be false (see [3] for details). I.Z. Ruzsa [2] has raised the question converse to that of Erdős':

Is it true that for every constant c there exists another constant c" such that for any finite $A \subset Z^1$

$$(1.5) \quad \frac{|A-A|}{|A|} \leq c \quad \text{implies} \quad \frac{|A+A|}{|A|} \leq c" \quad ?$$

Ruzsa answered both questions in the affirmative showing that $c' = c^2$ is good in (1.4), $c" = c^3$ is good in (1.5). He also showed that, denoting $\alpha := \log c'/\log c$ and $\beta := \log c"/\log c$, for these numbers we have asymptotically (i.e. when $c \to +\infty$), [2],

$$(1.6) \quad 1.2 < \alpha \leq 2, \; 1.02 < \beta \leq 3.$$

Similar asymptotic results for n-dimensional case have been proved in [7]. More precisely, in [7] lim-inf and lim-sup of the quantity $\log |A+A| / \log |A-A|$ when $|A| \to \infty$, are studied.

As to the structure of $A \subset Z^n$ when $|A-A|$ is small, the methods of [1] seem to be good to study this question, however some unexpected difficulties may arise in the course of adaptation (e.g., while the proof of (1.8) is almost trivial, that of (2.1) needs more care). The need for sharp lower estimations for $|A-A|$ in terms of $|A|$, when $A \subset \Lambda \subset R^n$, has been raised in [4], where the trivial inequality $|A-A| \geq 2|A| - 1$ is used to prove theorems sharpening the classical theorem of Minkowski-Blichfeldt in geometry of numbers (see [4], [5]). The

method can be used successfuly also in structures more general than R^n, [6]. We can state that the sharper estimation for $|A-A|$ we have, the sharper results in geometry of numbers can be proved (see Section 3 for details). More exactly, the following problem has been formulated in [4], [5]: Denoting by φ the canonical map of R^n into R^n/Λ, characterize the L-measurable sets $H \subset R^n$ such that

$$(1.7) \qquad |H \cap \omega - H \cap \omega| \geq r|H \cap \omega| - s$$

for all $\omega \in \varphi(H)$, where $r \geq 2$, $s \geq 0$ are constants. A "prototype" of characterization we have in mind is the following result proved for sum-sets, [1]: The (affine) dimension of the set $A \subset R^n$ is defined as the minimum of dimensions of flats containing the set.
If the dimension of $A \subset R^n$ is m then

$$(1.8) \qquad |A+A| \geq (m+1) \cdot |A| - \frac{m(m+1)}{2} \quad .$$

The mai result of this paper is that (1.8) is true also for $|A-A|$. This is proved in Section 2.
Section 3 is devoted to some possible sharpenings of the result and also to investigations of the equality in the inequality proved. The application of the results to geometry of numbers is also described in Section 3.

2. A LOWER BOUND FOR $|A - A|$

In this section we prove

THEOREM 2.1. If the affine dimension of $A \subset R^n$ is m, then

$$|A - A| \geq (m+1) \cdot |A| - \frac{m(m+1)}{2} \quad . \quad \square \tag{2.1}$$

To establish our inductive proof, first we prove a

LEMMA 2.1. If A spans the n-space then A can always be reduced by two points such that for the reduced set A' the inequality

$$|A - A| \geq |A' - A'| + 2(n+1) \tag{2.2}$$

holds. $\square$

PROOF OF THE LEMMA: Let $a_1, a_2, \ldots, a_k$ be the points of A where a_1 and a_k are two vertices of the convex hull of A such that they are unique points of A being on two parallel supporting hyperplanes of the convex hull. We can assume that $a_1 = -a_k$ (this can be achieved after a suitable translation of A). We shall denote the negative of an arbitrary point x by x'. Consider the set $B = A \cup (-A)$ and let C be the convex hull of B. Consider the edges of the polytope C that meet at a_1. On each of these edges there is a point of

B nearest to a_1. We denote these points by $b_1, b_2, \ldots, b_d$, where d is the degree of the vertex.

Since C is an n-dimensional polytope, $d \geq n$ holds and the edge-vectors $a_1 - b_i$, $i=1,\ldots,d$ are all different. Let S_i be a supporting hyperplane of C containing nothing of C but the edge e_i defined by a_1 and b_i and S_i' be its "negative" i.e. the supporting hyperplane parallel to S_i (and containing nothing but the edge e_i' defined by a_k and b_i').

If f_1 and f_2 are points of C such that $f_1 - f_2 = a_1 - b_i' = c_i$ then f_1 must lie on S_i and f_2 on S_2', more precisely, $f_1 \in e_i$ and $f_2 \in e_i'$. Consequently, the rest of the proof of our lemma reguires only a simple 2-dimensional analysis as follows:

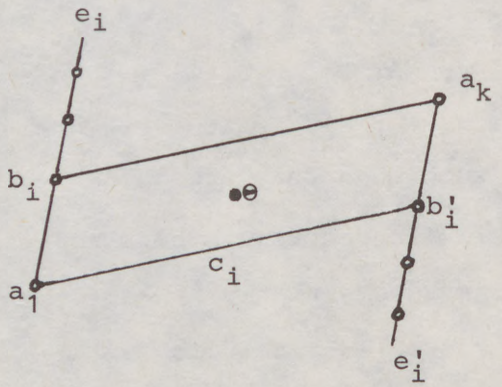

Figure 1.

It is clear (Fig. 1) that f_1 and f_2 must lie on the closed segment $[a_1, b_i]$ and $[b_i', a_k]$, respectively. On

the other hand we know that only the endpoints of these segments belong to B. Thus c_i has only two "representations" in B: $a_1 - b_i'$ and $b_i - a_k$. Consequently, as either b_i or b_i' belongs to A as well, the removal of a_1 and a_k from A reduces the cardinality of $|A - A|$ by at least 2d. That completes the proof of the lemma. □

Before the proof of the theorem let us note that

(2.4) $\quad |A - A| \geq 2|A| - 1$

and equality holds in (2.4) if and only if $A = \{a, a+f, a+2f, \ldots, a+(k-1)f\}$, where f is a lexicographically positive element. (Both (2.4) and equality criterium can be proved easily taking the points of A into lexicographic order.)

PROOF OF THE THEOREM. We can assume without the loss of generality that $m = n$. Let $k := |A|$. It is clear that $k \geq n+1$. The proof goes by induction on $n + k$. For $n = 1$ (2.1) is true for all k by (2.4). Assume that the theorem is true for all n and k such that $k \geq n+1$ and $n + k \leq N - 1$ and let n,k be such that $n + k = N$, $k \geq n + 1$. We shall distinguish three special cases.

CASE 1. If the convex hull of A is a pyramid, e.e. $(k - 1)$ points of A span a hyperplane and the remaining point, say a_k, is outside the hyperplane, then every

vector $a_k - a$, $a - a_k$, $a \in A' = \{A \backslash a_k\}$ is unique, hence $|A - A| \geq |A' - A'| + 2(k-1)$ and using the inductive hypothesis we get

$$(2.5) \qquad |A - A| \geq (n+1)k - \frac{n(n+1)}{2} + k - 2 \ .$$

We note that (2.5) is even sharper than (2.1).

CASE 2. Let the set $A \backslash \{a_1, a_k\}$, where a_1, a_k are the two points guaranteed by the lemma, be of the dimension $d < n$. If $d = n-2$ then for A we have the Case 1. Let $d = n-1$. The $a_1 - a_k$ and $-a_1 + a_k$ are unique, hence for the set $A' = A \backslash a_1$ we have $|A - A| \geq |A' - A'| + 2$ and applying to A' the Case 1 we get

$$(2.6) \qquad |A - A| \geq (n+1)k - \frac{n(n+1)}{2} + k - (n+2) \ .$$

We note that in this case $k \geq n+2$ must hold, hence (2.6) is again sharper than (2.1).

CASE 3. Assume that the convex hull of A is neither a pyramid nor the Case 2 holds. Then the set $A' = A \backslash \{a_1, a_k\}$, where a_1, a_k are the two points guaranteed by the lemma, is necessarily n-dimensional, hence applying the lemma and the inductive hypothesis we get (2.1). □

3. REMARKS, APPLICATIONS

In this section we first mention some possible sharpenings of (2.1). When looking for sharpenings, the emphasis is taken on improving the multiplying constant $(m+1)$ in (2.1) rather than the additive one $m(m+1)/2$. Let us consider a m-dimensional set D of points v_i $i=1,\ldots,k$ in R^n and let v be a vector not parallel to the m-dimensional flat spanned by D. It is easy to show that the cardinality of the difference set of the union E of D and $D+v$ is $3|D-D|$, i.e. to any finite set we can construct another one with twice as many points while increasing its dimension by one and tripling the cardinality of its difference set. To see this, notice that by projection along v the difference vectors of E are mapped onto the difference vectors of D. The first three of the four difference vectors $v_i - v_j$, $(v_i+v) - v_j$, $v_i - (v_j+v)$ and $(v_i+v) - (v_j+v)$ are all different and all mapped onto $v_i - v_j$. Thus we can say that to each 'old' difference vector there corresponds exactly 3 'new' ones.

Let us look more closely at the situation in R^3. If D is 1-dimensional then $|D-D| \geq 2k-1$. "Doubling" this set according to the above rule we get $|E-E| \geq 3(2k-1) = 3|E|-3$ and "doubling" E we finally get $|F-F| \geq 3(3|E|-3) = 9|F|/2 - 9 = 4.5|F| - 9$. We see that this configuration

yields "better" estimation than (2.1), in the sense that instead of $4|F|$ we have $4.5|F|$. We conjecture that for m-dimensional sets consisting of $2^m.t$ points the above construction supplies the "best" sets. The formula in (2.1) and the conjectured one coincide in the one and two-dimensional case and the second is sharper for every higher dimension. Our opinion that the proved lower estimation is not the 'real' one is supported by the fact that even for 3-dimensional case simple parity consideration show that the additive constant -6 can be replaced by -5.

In the remaining part of the section we briefly sketch the application of Theorem 2.1 to geometry of numbers mentioned in Sec. 1.

Let $\Lambda \subset R^n$ be a point lattice of full dimension and let P be one of its unit cells, i.e. a subset being in a one-to-one correspondence with the quotient space R^n/Λ. Usually $P = \{x \in R^n : x = \sum_{i=1}^{n} \lambda_i b_i,\ 0 \le \lambda_i < 1\}$, where $b_1, \ldots, b_n \in R^n$ is a basis of Λ. Then the canonical map $\varphi : R^n \to R^n/\Lambda \sim P$ is defined as

$$(3.1) \qquad \varphi(x) = \sum_{i=1}^{n} \{\xi_i\} b_i,\ x = \sum_{i=1}^{n} \xi_i b_i \in R^n ,$$

where $\{\xi_i\}$ is the fractional part of ξ_i, i.e. the number such that $0 \le \{\xi_i\} < 1$ and $\xi_i - \{\xi_i\}$ is integer. By definition, for any set $S \subset R^n$ $\varphi(S) := \bigcup_{x \in S} \varphi(x)$.

Now, for any set $S \subset R^n$ denote (see [4], [5], [6]).

$$(3.2) \qquad S_i := \{x \in P: |(S - x) \cap \Lambda| = i\}, \ i=0,1,2,\ldots \ .$$

One can see easily that $\varphi(S) = \bigcup_{i=1}^{\infty} S_i$.

Moreover, the following identities can be easily proved

$$(3.3) \qquad V(\varphi(S)) = \sum_{i=1}^{\infty} V(S_i) \ ,$$

$$(3.4) \qquad V(S) = \sum_{i=1}^{\infty} i \cdot V(S_i) \ .$$

(These identities hold in a much more general setting, see [6]).

The set S defines one more decomposition of $\varphi(S)$ as follows.

$$(3.5) \qquad S^{(j)} := \{x \in P: \dim((S - x) \cap \Lambda) = j\}, \ j=0,1,2,\ldots,n,$$

where dim(·) is the affine dimension of the set. It is clear that $\varphi(S) = \bigcup_{j=0}^{n} S^{(j)}$, consequently

$$(3.6) \qquad V(\varphi(S)) = \sum_{j=0}^{n} V(S^{(j)}) \ .$$

Now, we have

LEMMA 3.1. For any set $S \subset R^n$, if $S_i \cap S^{(j)} \neq \emptyset$, then

$$(3.7) \quad |(S-S) \cap \Lambda| \geq (j+1)i - \frac{j(j+1)}{2} . \quad \square$$

PROOF: The proof is an application of a simple idea used in [4] (see also [5], [6]) and (2.1). Namely, if $x \in S_i \cap S^{(j)}$, then $(S-x) \cap \Lambda \neq \emptyset$ and we can write

$$(3.8) \quad (S-S) \cap \Lambda \supseteq (S-x) \cap \Lambda - (S-x) \cap \Lambda ,$$

hence

$$(3.9) \quad |(S-S) \cap \Lambda| \geq |(S-x) \cap \Lambda - (S-x) \cap \Lambda| .$$

Applying (2.1) we get (3.7). $\square$

In spite of its simplicity, the lemma has an interesting consequence.

THEOREM 3.1. Let $S \subset R^n$ be a bounded Lebesgue-measurable set of positive L-measure $V(S)$. Then

$$(3.10) \quad |(S-S) \cap \Lambda| \geq (m+1) \cdot \frac{V(S)}{V(\varphi(S))} - \frac{M(M+1)}{2}$$

where $m := \min\{j : V(S^{(j)}) > 0\}$ and $M := \max\{j : V(S^{(j)}) > 0\}$. $\square$

PROOF: The identities (3.3), (3.4) and (3.6) show that if $V(S_i) > 0$ then there is $j(i)$ such that $V(S^{(j(i))}) > 0$ and $S_i \cap S^{(j(i))} \neq \emptyset$. For such a pair of indices we have by (3.7)

$$(3.11) \quad |(S-S)\cap\Lambda| \geq (j(i)+1)\, i - \frac{j(i)(j(i)+1)}{2}$$

and this implies

$$(3.12) \quad |(S-S)\cap\Lambda| \geq (m+1)\, i - \frac{M\,(M+1)}{2}$$

Using (3.4) we get (3.10). □

The inequality (3.10) is a useful extension of Theorem 2, [6], p. 936., where we had to assume the symmetry of the sets $(S-x)\cap\Lambda$, having had in hand the result (2.1) only for symmetric sets.

The inequality (3.10) can be compared also with the inequality

$$(3.13) \quad |(S-S)\cap\Lambda| \geq 2\,\frac{V(S)}{V(\varphi(S))} - 1$$

proved earlier in [4], [5], and in more general structures in [6].

Of course, the question, for what sets the right hand side of (3.10) is greater than that of (3.13), seems to

be worthy of study. In other words we have a problem to characterize those sets S for which

$$(3.14)\quad (m-1)\,\frac{V(S)}{V(\varphi(S))} > \frac{M(M+1)}{2} - 1 \quad .$$

Using (3.10) one can write statements of the following type (analogously to those in [6]):
"If $V(S)/V(\varphi(S)) > q$ then $S - S$ contains at least p lattice points."
In any case, the decompositions (3.3), (3.4) and (3.6) seem to be interesting also in themselves.

REFERENCES

[1] G. FREIMAN, "Foundations of a structural theory of set addition", *Am. Math. Soc.*, Providence, R.I., 1973.

[2] I.Z. RUZSA, On the cardinality of $A+A$ and $A-A$, In: A. Hajnal, V.T. Sós, Eds., "Combinatorics", Coll. Math. Soc. J. Bolyai, Vol 18, North-Holland, 1978, 933-938.

[3] I.Z. RUZSA, Sets of sums and differences, *Proc. of Seminaire de Théorie des nombres de Paris* (1982-1983), Birhäuser, Boston, 1984, 267-273.

[4] B. UHRIN, Some estimations useful in geometry of numbers, *Period. Math. Hungar.*, 11 (1980), 95-103.

[5] B. UHRIN, On a generalization of Minkowski convex body theorem, *J. of Number Th.*, 13 (1981), 192-209.

[6] B. UHRIN, Some remarks about the lattice points in difference sets, in: J. Szabados, Ed., "Proc. of A. Haar Memorial Conf. (Budapest, 1985)", *Coll. Math. Soc. J. Bolyai*, Vol. 49, North-Holland, Amsterdam-New York, 1986, 929-937.

[7] V.P. PIGAREV, G.A. FREIMAN, On the connection between the invariants R and T, In: "Number-theoretic Research on Markov Spectrum and the Structural Theory of Set Addition", State Univ. in Kalinin, Moscow, 1973, 172-174.

G. FREIMAN
Department of Mathematics, Tel-Aviv University
Ramat-Aviv, 69978 Tel-Aviv, Israel

A. HEPPES and B. UHRIN
Computer and Automation Institute, Hungarian Academy of Sciences
1502. Budapest, P.f. 63, Hungary

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

UNIFORM DISTRIBUTION OF THE ZEROS OF THE RIEMANN ZETA FUNCTION AND THE MEAN VALUE THEOREMS

FUJII A.

§ 1. INTRODUCTION

In the previous articles [1], [2], [3] cf. also References in [1] , the author has investigated on the uniform distribution of the zeros of the Riemann zeta function $\zeta(s)$. Here we are concerned with an application of some explicit versions of some of our previous results in [1]. We assume the Riemann Hypothesis throughout this article.

We start with recalling two theorems from [1]. Let γ run over the positive imaginary part of the zeros of $\zeta(s)$.

THEOREM A.

$$\sum_{0<\gamma\leqq T} e^{i\alpha\gamma} = -\frac{\Lambda(e^{\alpha})}{e^{\alpha/2}}\frac{T}{2\pi}+\frac{e^{i\alpha T}}{2\pi i\alpha}\log T + O\left(\frac{\log T}{\log\log T}\right),$$

where α is any positive constant, $T > T_0$ and $\Lambda(x)$ is the von Mangoldt function whose value is supposed to be 0 when x is not a natural number.

THEOREM B. For any positive constant α,

$$\lim_{T\to\infty}\frac{1}{T}\sum_{0<\gamma\leqq T} e^{i\gamma\log\left(\frac{\gamma}{2\pi e\alpha}\right)} = \begin{cases} -e^{\frac{1}{4}\pi i}\,\frac{C(\alpha)}{2\pi} & \text{if } \alpha \text{ is rational} \\ 0 & \text{if } \alpha \text{ is irrational,} \end{cases}$$

where we put $C(\alpha) = \frac{1}{\sqrt{\alpha}}\,\frac{\mu(q)}{\phi(q)}$ with the Möbius function $\mu(q)$ and the Euler function $\phi(q)$ if $\alpha = a/q$ with relatively prime integers a and $q \geqq 1$.

Theorem A is a refinement of Landau's theorem; for any $\alpha > 0$,

$$\sum_{0<\gamma\leqq T} e^{i\alpha\gamma} = -\frac{\Lambda(e^{\alpha})}{e^{\alpha/2}}\,\frac{T}{2\pi} + O(\log T).$$

Theorem B exhibits a connection of the distribution of γ with a rational number. These two theorems are the special cases of our more general theorem with the remainder term (Cf.[1]). We have left open a very interesting problem to prove that the sequence $a\gamma \log(\frac{\gamma}{2\pi e\ \alpha})$ is uniformly distributed mod one for any positive constants a and α , namely, to prove, by Weyl criterion, that

$$\sum_{0 < \gamma \leqq T} e^{2\pi i n\, a\, \gamma \log\left(\frac{\gamma}{2\pi e \alpha}\right)} = o\,(T \log T)$$

for any integer $n \geqq 1$.

On the other hand, Gonek [4] has recently shown the following mean value theorem;

$$\sum_{0<\gamma \leqq T} \left|\zeta\left(\frac{1}{2} + i\left(\gamma + \frac{2\pi\alpha}{\log \frac{T}{2\pi}}\right)\right)\right|^2$$

$$= \left(1 - \left(\frac{\sin\pi\alpha}{\pi\alpha}\right)^2\right) \frac{T}{2\pi} \log^2 T + O\,(T \log T),$$

where $T > T_o$ and α is a real number satisfying $|\alpha| \leqq \frac{1}{4\pi} \log \frac{T}{2\pi}$. Later in [5] he has given a different proof with the remainder term $O(T \log^{7/4} T)$. In this article we shall refine this as follows.

Theorem. Suppose that $T>T_0$ and $\Delta=\frac{2\pi\alpha}{\log\frac{T}{2\pi}}$ $(\neq 0)$ is bounded. Then

$$\sum_{0<\gamma\leq T} \left|\zeta\left(\frac{1}{2}+i\left(\gamma+\frac{2\pi\alpha}{\log\frac{T}{2\pi}}\right)\right)\right|^2$$

$$= \left(1-\left(\frac{\sin\pi\alpha}{\pi\alpha}\right)^2\right)\frac{T}{2\pi}\log^2\frac{T}{2\pi} + 2\left((1-2C_0)\frac{\sin(2\pi\alpha)}{2\pi\alpha}\right.$$

$$\left. + C_0 - 1 + \mathrm{Re}\left(\frac{\zeta'}{\zeta}(1+i\Delta)\right)\right)\frac{T}{2\pi}\log\frac{T}{2\pi}$$

$$+ G(T,\alpha) + O(T^{9/10}\log^2 T),$$

where C_0 is the Euler constant, $G(T,\alpha)$ will be described explicitly below and the remainder term does not depend on α.

To describe $G(T,\alpha)$, we introduce some notations.

$$R(y) = \sum_{n\leq y}\Lambda(n) - y .$$

$$R_1(y) = \sum_{n\leq y}\sum_{k|n}\Lambda(k)k^{i\Delta} + y\frac{\zeta'}{\zeta}(1-i\Delta) - \frac{y^{1+i\Delta}}{1+i\Delta}\zeta(1+i\Delta).$$

We remark that $R_1(y)\ll y^{\frac{1}{2}+\varepsilon}$, where ε denotes (always in this article) an arbitrarily small positive number

(Cf. Lemma in the section 3 below). Now

$$G(T,\alpha)=-\frac{T}{\pi}\,\mathrm{Re}\Big(C_o-1+\frac{\zeta'}{\zeta}(1+i\Delta)+(1+i\Delta)\int_1^\infty \frac{R(y)}{y^{2+i\Delta}}\,dy+$$

$$+2\int_1^\infty \frac{R_1(y)}{y^2}+2^{2+i\Delta}Q\sum_{\ell=1}^{\infty}(\pi\ell)^{i\Delta}\int_{2\pi\ell}^{\infty}\frac{\cos w}{w^{3+i\Delta}}\,dw-$$

$$-2\Big(\zeta(1+i\Delta)-\frac{1}{i\Delta}\Big)\frac{Q}{2+i\Delta}+2\Big(\zeta(1+i\Delta)-\frac{1}{i\Delta}-C_o\Big)\cdot$$

$$\cdot\Big(\frac{Q-1}{i\Delta}-\frac{Q}{(1+i\Delta)\,i\Delta}\Big)+\frac{5}{6}\cdot\frac{Q}{2+i\Delta}+\frac{1}{1+\Delta^2}+$$

$$+(2C_o-1)(Q-Q^2)/(1+i\Delta)+\Big(\zeta^2(1+i\Delta)+\frac{1}{\Delta^2}-\frac{2C_o}{i\Delta}\Big)Q^2/(1+i\Delta),$$

where $Q=(T/2\pi)^{i\Delta/2}$.

We remark that $G(T,\alpha)<<T$.

To prove our Theorem we shall use the Riemann-Siegel formula and explicit versions of Theorems A and B which will be stated as follows.

Theorem A'. Let $0<Y_o<Y\leq T$. Then

$$\sum_{Y_o<\gamma\leq Y} e^{i\alpha\gamma} = A(\alpha, Y, Y_o) + O\Big((\alpha e^{\frac{1}{2}\alpha}+1)\,\frac{\log Y}{\log\log Y}\Big)$$

$$-\frac{\alpha}{2\pi}\sum_{k=2}^{\infty}\frac{\Lambda(k)}{k^{1+\delta}\log k}\,e^{(\frac{1}{2}+\delta)\alpha}\int_{Y_o}^{Y} e^{-it\log k+it\alpha}\,dt$$

$$- \frac{\alpha}{2\pi} \sum_{k=2} \frac{\Lambda(k)}{k^{1+\delta} \log k} e^{-(\frac{1}{2}+\delta)\alpha} \int_{Y_o}^{Y} e^{it \log k + it\alpha} \, dt$$

uniformly for a positive α, where we put $\delta = 1/\log T$ and

$$A(\alpha, Y, Y_o) = \frac{e^{i\alpha Y}}{2\pi i \alpha} \log \frac{Y}{2\pi} - \frac{e^{-i\alpha Y_o}}{2\pi i \alpha} \log \frac{Y_o}{2\pi} +$$

$$+ O\left(\mathrm{Min}\left(\frac{\log Y}{\alpha^2}, \frac{1}{\alpha^3}\right)\right)$$

$$\text{or } A(\alpha, Y, Y_o) = O\left(\frac{\log Y}{\alpha}\right).$$

Theorem B'. Let m and n be integers satisfying $1 \leqq m \leqq n$ and q be an integer $\geqq 1$. Suppose that $2\pi n^2/q \leqq Y \leqq T$. Then

$$\sum_{2\pi n^2/q < \gamma \leqq Y} e^{i\gamma \log(q\gamma/2\pi emn)}$$

$$= - e^{\frac{1}{4}\pi i} \sqrt{\frac{mn}{q}} \sum_{n/m < k < Yq/2\pi mn} \Lambda(k) e^{-\frac{2\pi imnk}{q}} +$$

$$+ O\left(\sqrt{\frac{mn}{q}} \sum_{n/m \leqq k \leqq n/m(1-\nu)} \Lambda(k)\right)$$

$$+ O\Big(\sqrt{\frac{mn}{q}} \sum_{Yq/(1+\nu)2\pi mn \leq k \leq Yq/2\pi mn} \Lambda(k)\Big)$$

$$+ O\Big(\sqrt{\frac{Yq}{mn}} \ (T^{2/5} + (\log qT)^4\Big) + \delta_{n,m}\, O\Big(\frac{n}{\sqrt{q}} \log Y\Big)$$

$$+ \ (1 - \delta_{n,m}) O\Big(\frac{\log Y}{\log(n/m)}\Big),$$

where we put $\nu = T^{-2/5}$, $\delta_{n,m} = 1$ if $m = n$ and $\delta_{n,m} = 0$ otherwise.

Since the proofs of Theorems A′ and B′ are implicit in [1] , we shall omit them.

We remark that in a similar manner we can treat the sums like

$$\sum_{0<\gamma \leq T} \zeta'(\tfrac{1}{2} + i\gamma), \quad \sum_{0< \gamma \leq T} L(\tfrac{1}{2} + i\,\gamma, \chi)$$

and

$\sum_{0< \gamma \leq T} |L(\frac{1}{2} + i\gamma, \chi)|^2$, where $L(s,\chi)$ is a Dirichlet L-function. These will appear elsewhere.

We shall prove our theorem in the two steps. First, in the section 2, we shall give an explicit formula for

the sum using the Riemann-Siegel formula, Theorems A' and B'. In the section 3 we shall evaluate each term which appears in the explicit formula, combine them and complete the proof of our theorem.

§ 2. EXPLICIT FORMULA FOR THE SUM IN THEOREM

We shall use the following well-known Riemann-Siegel formula (Cf. 4.17.4 of [8]).

$$e^{i\Theta}\zeta(\tfrac{1}{2}+it)=2\sum_{1\le n\le\sqrt{t/2}}\frac{\cos(\Theta-t\log n)}{\sqrt{n}}+O(t^{-\frac{1}{4}}),$$

where $t>t_o$ and

$$\Theta\equiv\Theta(t)=\tfrac{1}{2}t\log\frac{t}{2\pi}-\tfrac{1}{2}t-\tfrac{1}{8}\pi+O(1/t)$$

$$=\Theta_1(t)+O(1/t),\ \text{say.}$$

Using this formula, our sum is written as

$$\sum_{0<\gamma\le T}|\zeta(\tfrac{1}{2}+i(\gamma+\Delta))|^2$$

$$=4\sum_{0<\gamma\le T}\sum_{1\le m,n\le\sqrt{(\gamma+\Delta)/2\pi}}\frac{\cos(\Theta_1(\gamma+\Delta)-(\gamma+\Delta)\log n)}{\sqrt{mn}}$$

$$.\cos(\Theta_1(\gamma+\Delta)-(\gamma+\Delta)\log m)$$

$$+ O\Big(\sum_{0<\gamma \leq T} \gamma^{-\frac{1}{4}} \Big| \sum_{1\leq n\leq \sqrt{(\gamma+\Delta)/2\pi}} \frac{\cos(\theta_1(\gamma+\Delta)-(\gamma+\Delta)\log n)}{\sqrt{n}} \Big| \Big)$$

$$+ O\Big(\sum_{0<\gamma\leq T} \gamma^{-\frac{1}{2}} \Big)$$

$$= S_1 + S_2 + S_3, \text{ say.}$$

$$S_3 << \sum_{1\leq k\leq T} \frac{1}{\sqrt{k}} \sum_{k<\gamma\leq k+1} . \quad 1 << \sqrt{T}\log T.$$

$$S_2 << S_1^{\frac{1}{2}} \; T^{\frac{1}{4}} \; (\log T)^{\frac{1}{2}} .$$

S_1 can be further rewritten as follows.

$$S_1 = 2\,\mathrm{Re}\Big(e^{-\frac{1}{4}\pi i} \sum_{0<\gamma\leq T} \sum_{1\leq m,n\leq\sqrt{(\gamma+\Delta)/2\pi}} \frac{e^{i\gamma\log(\frac{\gamma}{2\pi emn})}\, e^{i\Delta\log\frac{\gamma}{2\pi}}}{\sqrt{mn}\;(mn)^{i\Delta}}\Big)$$

$$+ 2 \sum_{0<\gamma\leq T} \sum_{1\leq m,n\leq\sqrt{(\gamma+\Delta)/2\pi}} \frac{e^{i\gamma\log\frac{n}{m}}}{\sqrt{mn}} \Big(\frac{n}{m}\Big)^{i\Delta}$$

$$+ O\Big(\sum_{0<\gamma\leq T} \frac{1}{\gamma} \sum_{1\leq m,n\leq\sqrt{(\gamma+\Delta)/2\pi}} (mn)^{-1/2}\Big)$$

$$= 2\,\mathrm{Re}(S_4) + 2S_5 + O(S_6), \text{ say.}$$

$S_6 << \sqrt{T} \log T.$

$$S_4 = 2\, e^{-\frac{1}{4}\pi i} \sum_{1\leq m<n\leq T_1} (mn)^{-\frac{1}{2}-i\Delta} \sum_{2\pi n^2 \leq \gamma \leq T} e^{i\Delta \log \frac{\gamma}{2\pi}}$$

$$\cdot e^{i\gamma \log \left(\frac{\gamma}{2\pi emn}\right)}$$

$$+ e^{-\frac{1}{4}\pi i} \sum_{1\leq n\leq T_1} n^{\frac{1}{1+2i\Delta}} \sum_{2\pi n^2 \leq \gamma \leq T} e^{i\Delta \log \frac{\gamma}{2\pi}}$$

$$\cdot e^{i\gamma \log \frac{\gamma}{2\pi e n^2}}$$

$$+ O(\sqrt{T} \log T)$$

$$= 2\, e^{-\frac{1}{4}\pi i} S_7 + e^{-\frac{1}{4}\pi i} S_8 + O(\sqrt{T} \log T), \text{ say, where}$$

we put $T_1 = \sqrt{T/2\pi}$.

Using Theorem B', we get easily,

$$2\, e^{-\frac{1}{4}\pi i} S_7 = -2 \sum_{m<n\leq T_1} \sum_{n/m<k<T/(2\pi mn)} \Lambda(k) k^{i\Delta}$$

$$+ O(T^{9/10} \log^2 T).$$

Similarly, we obtain

$$e^{-\frac{1}{4}\pi i} S_8 = -\sum_{n \leq T_1} \sum_{k < T/(2\pi n^2)} \Lambda(k)\, k^{i\Delta} + O(T^{9/10}).$$

We shall next evaluate S_5.

$$S_5 = \sum_{1 \leq m \leq T_1} \frac{1}{m} \sum_{2\pi m^2 \leq \gamma \leq T} 1.$$

$$+ 2\,\mathrm{Re}\Big(\sum_{1 \leq m < n \leq T_1} (mn)^{-\frac{1}{2}} \Big(\frac{n}{m}\Big)^{i\Delta} \sum_{2\pi n^2 \leq \gamma \leq T} e^{i\gamma \log \frac{n}{m}}\Big)$$

$$+ O(\sqrt{T} \log T)$$

$$= S_9 + 2\,\mathrm{Re}(S_{10}) + O(\sqrt{T} \log T), \text{ say.}$$

By Riemann- von Mangoldt formula (Cf. Theorem 9.4 of [8]), we get

$$S_9 = \frac{1}{2} \frac{T}{2\pi} \Big(\log \frac{T}{2\pi}\Big)^2 + \frac{T}{2\pi} \log \frac{T}{2\pi} (C_o - 1) - \frac{T}{2\pi}(C_o - 1)$$
$$+ O(\sqrt{T} \log T).$$

Using Theorem A', we get easily,

$$S_{10} = -\frac{T}{2\pi} \sum_{n \leqq T_1} \frac{1}{n} \sum_{k|n} \Lambda(k) k^{i\Delta}$$

$$+ \sum_{n \leqq T_1} n \sum_{k|n} \Lambda(k) k^{i\Delta} + O(T^{\frac{1}{2}+\varepsilon}).$$

Combining all the above evaluations, we get the following

THEOREM D. Let $T > T_o$ and $\Delta = \frac{2\pi\alpha}{\log \frac{T}{2\pi}}$ be bounded. Then we have

$$\sum_{0 < \gamma \leqq T} |\zeta(\tfrac{1}{2} + i(\gamma+\Delta))|^2$$

$$= \frac{T}{2\pi} (\log \frac{T}{2\pi})^2 + \frac{1}{\pi} T \log \frac{T}{2\pi} (C_o - 1) - \frac{1}{\pi} T (C_o - 1)$$

$$- \frac{T}{\pi} \sum_{n \leqq T_1} \frac{1}{n} \sum_{k|n} \Lambda(k) (k^{i\Delta} + k^{-i\Delta})$$

$$+ 2 \sum_{n \leq T_1} \; \sum_{k \mid n} \Lambda(k)\,(k^{i\Delta} + k^{-i\Delta})$$

$$- 2 \sum_{1 \leq m < n \leq T_1} \; \int_{n/m < k < T/(2\pi mn)} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$- \sum_{n \leq T_1} \; \sum_{k \leq T/(2\pi n^2)} \Lambda(k)\,(k^{i\Delta} + k^{-i\Delta})$$

$+ O(T^{9/10} \log^2 T)$, where we put $T_1 = \sqrt{T/2\pi}$.

§ 3. EVALUATION OF EACH TERM IN THEOREM D AND THE COMPLETION OF THE PROOF OF THEOREM

For simplicity, we put $N = [T/2\pi]$.

Since

$$\sum_{2\pi N < \gamma \leq T} \left|\zeta\left(\frac{1}{2} + i\,(\gamma + \Delta)\right)\right|^2$$

$$\ll T^{\varepsilon} \sum_{2\pi N \leq \gamma \leq T} 1 \ll T^{\varepsilon}$$, we have

$$\sum_{0 < \gamma \leq T} \left|\zeta\left(\frac{1}{2} + i(\gamma + \Delta)\right)\right|^2$$

$$= N \log^2 N + 2N \log N\,(C_0 - 1) - 2N(C_0 - 1)$$

$$- 2N \sum_{n \leq \sqrt{N}} \frac{1}{n} \sum_{k|n} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$+ 2 \sum_{n \leq \sqrt{N}} n \sum_{k|n} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$- 2 \sum_{1 \leq m < n \leq \sqrt{N}} \sum_{n/m < k < N/mn} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$- \sum_{1 \leq n \leq \sqrt{N}} \sum_{1 \leq k \leq N/n^2} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$+ O(T^{9/10} \log^2 T)$$

$$= N \log^2 N + 2N \log N \, (C_o - 1) - 2N(C_o - 1)$$

$$+ K_1 + K_2 + K_3 + K_4 + O(T^{9/10} \log^2 T), \text{ say.}$$

We suppose that $\Delta \neq 0$. By the prime number theorem with the remainder term $R(y) \ll y^{\frac{1}{2}} \log^2 y$, we get first

$$K_4 = - \frac{1}{1+i\Delta} N^{1+i\Delta} \zeta(2+2i\Delta) - \frac{1}{1-i\Delta} N^{1-i\Delta} \zeta(2-2i\Delta)$$

$$+ O(\sqrt{N} \log^3 N).$$

We shall next evaluate K_3.

$$K_3 = -2 \sum_{1 \leq m < n \leq \sqrt{N}} \sum_{k < N/mn} \Lambda(k) (k^{i\Delta} + k^{-i\Delta})$$

$$+ 2 \sum_{1 \leq m < n \leq \sqrt{N}} \sum_{k \leq n/m} \Lambda(k) (k^{i\Delta} + k^{-i\Delta})$$

$$= - 2K_5 + 2K_6, \text{ say.}$$

We shall evaluate K_6 first.

$$K_6 = \sum_{k \leq \sqrt{N}} \Lambda(k) (k^{i\Delta} + k^{-i\Delta}) \sum_{n \leq \sqrt{N}} \sum_{m \leq n/k} .1$$

$$= \sum_{k \leq \sqrt{N}} \frac{\Lambda(k)}{k} (k^{i\Delta} + k^{-i\Delta}) \sum_{n \leq \sqrt{N}} n$$

$$- \sum_{k \leq \sqrt{N}} \Lambda(k) (k^{i\Delta} + k^{-i\Delta}) \sum_{n \leq \sqrt{N}} (\{\frac{n}{k}\} - \frac{1}{2})$$

$$- \frac{1}{2}\sqrt{N} \sum_{k \leq \sqrt{N}} \Lambda(k) (k^{i\Delta} + k^{-i\Delta}) + 0(\sqrt{N})$$

$= B_1 + B_2 + B_3 + 0(\sqrt{N})$, where $\{x\}$ is the fractional part of x.

$$B_1 = \frac{N}{2}\left(\frac{\sqrt{N}^{\,i\Delta}}{i\Delta} - \frac{\sqrt{N}^{-i\Delta}}{i\Delta} - (1+i\Delta)\int_1^{\infty}\frac{R(y)}{y^{2+i\Delta}}\,dy\right.$$

$$\left. - (1-i\Delta)\int_1^{\infty}\frac{R(y)}{y^{2-i\Delta}}\,dy\right)$$

$$+ O(\sqrt{N}\log^2 N).$$

$$B_3 = -\frac{1}{2}\,\frac{N^{1+\frac{1}{2}i\Delta}}{1+i\Delta} - \frac{1}{2}\,\frac{N^{1-\frac{1}{2}i\Delta}}{1-i\Delta} + O(N^{3/4}\log^2 N).$$

Putting $L = N^{\frac{1}{4}}$, we get

$$B_2 = \sum_{k\le\sqrt{N}} \Lambda(k)\,(k^{i\Delta}+k^{-i\Delta}) \sum_{\substack{n\le\sqrt{N}\\ k\nmid n}} \sum_{\ell=1}^{L} \frac{\sin(2\pi\ell\,\frac{n}{k})}{\pi\ell}$$

$$+ O(N^{3/4}\log N)$$

$$= \sum_{k\le\sqrt{N}} \Lambda(k)\,(k^{i\Delta}+k^{-i\Delta}) \sum_{\ell=1}^{L} \frac{1}{\pi\ell}\int_0^{\sqrt{N}} \sin(2\pi\tfrac{\ell}{k}y)\,d(y-\{y\})$$

$$+ O(N^{3/4}\log N)$$

$$=- \sum_{\ell=1}^{L} \frac{1}{2\pi^2 \ell^2} \int_1^{\sqrt{N}} (y^{1+i\Delta} + y^{1-i\Delta}) \cos(2\pi \frac{\ell}{y}\sqrt{N}) d(y+R(y))$$

$$+ \frac{1}{2\pi^2}(\zeta(2)+0(1/L)) \int_1^{\sqrt{N}} (y^{1+i\Delta} + y^{1-i\Delta}) \, d(y+R(y))$$

$$+ \; 0(N^{3/4} \log N)$$

$$= - 2 \, \mathrm{Re}(2^{1+i\Delta} N^{1+\frac{1}{2}i\Delta} \sum_{\ell=1}^{\infty} (\pi\ell)^{i\Delta} \int_{2\pi\ell}^{\infty} \frac{\cos w}{w^{3+i\Delta}} \, dw)$$

$$+ \frac{\zeta(2)}{2\pi^2} \, 2 \, \mathrm{Re}(\frac{N^{1+\frac{1}{2}i\Delta}}{2+i\Delta}) + 0(N^{3/4} \log^3 N).$$

We next evaluate K_5.

$$2K_5 = \sum_{m \leq \sqrt{N}, \; n \leq \sqrt{N}} \; \sum_{k<N/mn} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$- \sum_{m \leq \sqrt{N}} \; \sum_{k<N/m^2} \Lambda(k)(k^{i\Delta} + k^{-i\Delta})$$

$$= (D_1 + \overline{D}_1) + (D_2 + \overline{D}_2), \text{ say.}$$

As before

$$D_2 = - \frac{N^{1+i\Delta}}{1+i\Delta} \zeta(2+2i\Delta) + O(\sqrt{N} \log^3 N).$$

To treat D_1, we put $U = N^{1/3}$ and $\beta = 1 + \frac{1}{\log T}$.

Then

$$D_1 = - \frac{1}{2\pi i} \int_{\beta-iU}^{\beta+iU} \Big(\sum_{m \le \sqrt{N}} \frac{1}{m^s}\Big) \Big(\sum_{n \le \sqrt{N}} \frac{1}{n^s}\Big) \frac{\zeta'}{\zeta}(s-i\Delta) \frac{N^s}{s} \, ds$$

$$+ O(N^{2/3 + \varepsilon})$$

$$= - \frac{1}{2\pi i} \int_{\beta-iU}^{\beta+iU} \frac{\zeta'}{\zeta}(s-i\Delta) \Big(\zeta^2(s) - 2\zeta(s) \frac{\sqrt{N}^{1-s}}{s-1}$$

$$+ \frac{N^{1-s}}{(1-s)^2}\Big) \frac{N^s}{s} \, ds + O(N^{5/6} \log^2 T).$$

Using the residue theorem, this is

$$= - 2N^{1+\frac{1}{2}\Delta i} \frac{\zeta(1+i\Delta)}{(1+i\Delta)\, i\Delta} + \frac{N^{1+i\Delta}}{1+i\Delta} \zeta^2(1+i\Delta)$$

$$+ \frac{N}{(1+i\Delta)\,(i\Delta)^2} + O(N^{\frac{7}{8} + \varepsilon}).$$

We have left the evaluations of K_1 and K_2. To do this we remark the following

LEMMA. Let $X>X_o$ and $\Delta\neq 0$. Then

$$\sum_{n\leq x} \sum_{k|n} \Lambda(k)k^{i\Delta} = -X\,\frac{\zeta'}{\zeta}(1-i\Delta) + \frac{X^{1+i\Delta}}{1+i\Delta}\,\zeta(1+i\Delta)+R_1(X),$$

where $R_1(X)<<X^{\frac{1}{2}+\varepsilon}$.

To prove this we remark only that the generating function is

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{k|n} \Lambda(k)k^{i\Delta} = -\frac{\zeta'}{\zeta}(s-i\Delta)\,\zeta(s) \quad \text{for } \mathrm{Re}(s)>1.$$

Using this lemma and the Stieltjes integral, we get

$$K_1 = N\log N\left(\frac{\zeta'}{\zeta}(1-i\Delta) + \frac{\zeta'}{\zeta}(1+i\Delta)\right)$$

$$-2N\zeta(1+i\Delta)\,\frac{N^{\frac{1}{2}i\Delta}-1}{i\Delta} - 2N\,\zeta(1-i\Delta)\,\frac{N^{-\frac{1}{2}i\Delta}-1}{-i\Delta}$$

$$-2N\int_1^{\infty} \frac{R_1(y)+\overline{R_1(y)}}{y^2}\,dy + O(N^{\frac{3}{4}+\varepsilon}).$$

$$K_2 = -N\left(\frac{\zeta'}{\zeta}(1-i\Delta) + \frac{\zeta'}{\zeta}(1+i\Delta)\right)$$

$$+ \frac{2N}{2 + i\Delta}\,\zeta(1+i\Delta) + \frac{2N}{2-i\,\Delta}\,\zeta(1-i\Delta) + O(N^{\frac{3}{4}+\varepsilon}).$$

Combining all the above estimates, replacing N by $T/2\pi$ in the remainder term and simplifying, we get the expressions in the Theorem, which completes the proof.

REFERENCES

[1] A. FUJII, On the uniformity of the distribution of the zeros of the Riemann zeta function (II), *Comment. Math. Univ. St. Pauli*, 31 (1), 99-113(1982).

[2] A. FUJII, Zeros, primes and rationals, *Proc. of Japán Academy* 58 Ser. A, 373-376(1982).

[3] A. FUJII, The zeros of the Riemann zeta function and Gibbs's phenomenon, *Comment. Math. Univ. St. Pauli*, 32 (2) 229-248(1983).

[4] S.M. GONEK, Mean values of the Riemann zeta function and its derivatives, *Invent. Math.* 75, 123-141 (1984).

[5] E.C. TITCHMARSH, A formula of Landau and mean values of $\zeta(s)$. *Topics in Analytic Number Theory*, University of Texas Press, 92-97 (1985).

[6] G.H. HARDY and J.E. LITTLEWOOD, Contributions to the theory of the Riemann zeta function and the theory of the distribution of primes, *Acta Math.*41 119-196 (1918).

[7] E. LANDAU, Über die Nullstellen der ζ -Funktion, *Math. Ann.* 71, 548-569(1911).

[8] E.C. TITCHMARSH, *The theory of the Riemann zeta function*, Oxford 1951.

FUJII, A.

Department of Mathematics
Rikkyo University
Tokyo, J a p a n

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

SUMS OF THREE SQUARE-FULL NUMBERS

D.R. HEATH-BROWN

An integer $n \geq 0$ is said to be square-full (or power-full) if $p|n$ implies $p^2|n$ for every prime p. Thus n is square-full if and only if it can be written as $n=a^2b^3$. In particular every square is square-full. In the 1970's Erdős and Ivić conjectured, independently, that every sufficiently large positive integer is a sum of three square-full numbers. Indeed Ivić calculated that every $n \leq 32000$, with the exceptions of $n = 7$, 15, 23, 87, 111 and 119, can be so represented.

The question raised be Erdős and Ivić is answered by the following result.

THEOREM 1. *There is an effectively computable constant n_0 such that every $n \geq n_0$ is a sum of three square-full numbers.*

A full proof of this may be found in Heath-Brown [1]. We content ourselves here with a discussion of the methods involved.

Legendre's Three Squares Theorem states that every $n \geq 0$ not of the form $n = 4^k(8l + 7)$ is a sum of three squares. It follows that if $2^e \| n$ with e odd, or if $n \equiv 1, 3$ or $5 \pmod 8$, then n can be written as $x^2 + y^2 + z^2$. It also follows that if $2^e \| n$ with $e > 0$ even, then $n = x^2 + y^2 + 8z^2$. Thus we immediately see that any $n \not\equiv 7 \pmod 8$ is a sum of three square-full numbers.

For the remaining integers we have the following conjecture.

CONJECTURE. *The quadratic form* $x^2 + y^2 + 125z^2$ *represente any sufficiently large integer* $n \equiv 7 \pmod 8$.

For the above form there is more than one class per genus, so that there is no simple representation theory. Partial results can be obtained by Linnik's "ergodic method". Thus, if we write $\chi_k(d)$ for the character $(\frac{k}{d})$, then a large integer $n \equiv 7 \pmod 8$ can be expressed as $x^2 + y^2 + 125z^2$, providing that the Dirichlet L-function $L(x, \chi_{-5n})$ does not vanish in the disc

$$(1) \qquad |s - 1| \leq \frac{(\log\log n)^2 \log\log\log n}{(\log n)^{1/2}} \quad .$$

This result is due to Malyšev [3].

In order to obtain an unconditional theorem we use a number of forms $x^2+y^2+p^3z^2$, with primes $p \equiv 5 \pmod 8$. Malyšev's work applies to these also, so that it would suffice for any of the resulting L-functions to have a zero-free disc (1).
Unfortunately, known zero-density theorems appear to be too weak to handle the resulting situation.

Instead we use an alternative approach due to Hooley [2].

THEOREM 2. *Let*

$$r(n,p) = \#\{(x,y,z) \in \mathbb{Z}^3 : n = x^2+y^2+p^3z^2\} .$$

Then for any $\varepsilon > 0$ *we have*

$$r(n,p) = S_p\, n(n)^{1/2} + $$

$$+ O_{\varepsilon,p}\left\{\frac{n^{1/2}}{(\log n)^{1-\varepsilon}} \{1+(\log n)^c L(1+\frac{1}{\log n}, \chi_{pn})^c\}\right\} ,$$

where $c = \frac{1}{2} + \frac{1}{\pi}$, *and the "singular series"* $S_p(n)$ *satisfies*

$$S_p(n) \gg_p (\log\log n)^{-2} L(1,\chi_{-pn}) .$$

Note that the implied constants above may depend on p. Since $0 < c < \frac{32}{39}$, it follows from Theorem 2 that $r(n,p) > 0$ whenever

$$L(1,\chi_{-pn}) \geq (\log n)^{-1/9} ,$$

$$L(1+\frac{1}{\log n}, \chi_{pn}) \leq (\log n)^{1/12} ,$$

and $n \geq n_p$. It may be observed that, in contrast to Malyšev's work, a condition on $L(s,\chi_{pn})$ is needed. This is a defect of the method.

To deduce Theorem 1 from Theorem 2 we use the following result.

THEOREM 3. *Let* S *be a set of odd primes, with* $\#S \geq 255026$. *Then there is a constant* $n(S)$ *such that, for any* $n \geq n(S)$, *there exists* $p \in S$ *with*

$$L(1,\chi_{-pn}) \geq (\log n)^{-1/19} ,$$

$$L(1+\frac{1}{\log n}, \chi_{pn}) \leq (\log n)^{1/12} .$$

The proof of Theorem 2 starts by writing

$$\sum_{|z|<n^{1/2}p^{-3/2}} r(n - p^3z^2)$$

$$= 4\sum_d \chi_{-1}(d) \quad \#\{z : |z| < n^{1/2} p^{-3/2},\ p^3z^2 \equiv n \pmod d\} ,$$

where

$$r(m) = \#\{x^2 + y^2 = m\} = 4 \sum_{d|m} \chi_{-1}(d) \quad .$$

The critical size for d turns out to be $d \approx n^{1/2}$, in which case the range for z is of length 0(d). One needs to know that the solutions of

$$(2) \qquad p^3 z^2 \equiv n \pmod{d}$$

are uniformly distributed (mod d). Of course, if d is prime there are 0(1) solutions z(mod d), so that they cannot be uniformly distributed. However almost all numbers have many prime factors, and for such numbers Hooley's method shows that the solutions of (2) are indeed well distributed.

To illustrate the proof of Theorem 3 we shall consider the following simpler result.

THEOREM 4. *If* S *is a set of primes, with* $\# S = N$, *then*

$$\min_{p \in S} |\log L(1 + \frac{1}{\log n}, \chi_{pn})| \leq \frac{\log\log n}{N^{1/4}} + 0_S(1) \quad .$$

For the proof it is convenient to write $s = 1 + \frac{1}{\log n}$. Our starting point is the formula

$$\log L(s, \chi) = \sum_{m=1}^{\infty} \Lambda_1(m) m^{-s} \chi(m) \quad ,$$

where

$$\Lambda_1(m) = \begin{cases} e^{-1}, & m = p^e \ , \\ 0 \ , & \text{otherwise.} \end{cases}$$

Since $\chi_{pn}(m) = \chi_p(m)\chi_n(m)$ we have

$$\min_{p \in S} (\log L(s, \chi_{pn}))^2 \leq \frac{1}{N} \sum_{p \in S} (\log L(s, \chi_{pn}))^2$$

$$= \frac{1}{N} \sum_{m_1, m_2 = 1}^{\infty} \frac{\Lambda_1(m_1)\Lambda_1(m_2)}{(m_1 m_2)^s} \chi_n(m_1 m_2) \sum_{p \in S} \chi_p(m_1 m_2) \tag{3}$$

$$\leq \frac{1}{N} \sum_{m_1, m_2 = 1}^{\infty} \frac{\Lambda_1(m_1)\Lambda_1(m_2)}{(m\, m_2)^s} \left| \sum_{p \in S} \chi_p(m_1 m_2) \right| \ .$$

Notice how the character χ_n no longer appears. The cancellation implied by Theorem 4 is due solely to the characters χ_p.

We now write

$$Q = \prod_{p \in S} p \quad ,$$

so that (3) becomes

$$\frac{1}{N} \sum_{a_1,a_2=1}^{Q} \Big| \sum_{p\in S} \chi_p(a_1a_2) \Big|$$

(4)

$$\prod_{i=1,2} \left\{ \sum_{m\equiv a_i (\mathrm{mod}\ Q)} \frac{\Lambda_1(m)}{m^s} \right\} .$$

However

$$\sum_{m\equiv a(\mathrm{mod}\ Q)} \frac{\Lambda_1(m)}{m^s} \ll_Q 1$$

if $(a,Q) \neq 1$, while for $(a,Q) = 1$ we have

$$\sum_{m\equiv a(\mathrm{mod}\ Q)} \frac{\Lambda_1(m)}{m^s} = \frac{1}{\varphi(Q)} \sum_{\chi(\mathrm{mod}\ Q)} \bar{\chi}(a) \log L(s,\chi)$$

$$= \frac{1}{\varphi(Q)} \log L(s,\chi_0) + 0_Q(1)$$

$$= \frac{1}{\varphi(Q)} \operatorname{loglog} n + 0_S(1) \quad ,$$

where χ_0 is the principal character (mod Q). The expression (4) therefore becomes

$$\frac{(\operatorname{loglog} n)^2}{N\varphi(Q)^2} \sum_{a_i=1}^{Q}{}^{*} \Big| \sum_{p\in S} \chi_p(a_1a_2) \Big| + 0_S(\operatorname{loglog} n) ,$$

where Σ^* denotes the condition $(a,Q) = 1$. According to Cauchy's inequality, the double sum above is

$$\varphi(Q) \sum_{a=1}^{Q}{}^{*} \left| \sum_{p \in S} \chi_p(a) \right| \leq \varphi(Q)^{3/2} \left\{ \sum_{a=1}^{Q}{}^{*} \left| \sum_{p \in S} \chi_p(a) \right|^2 \right\}^{1/2}$$

(5)

$$= \varphi(Q)^{3/2} \left\{ \sum_{p_1, p_2 \in S} \sum_{a=1}^{Q}{}^{*} \chi_{p_1 p_2}(a) \right\}^{1/2}.$$

One readily checks that the inner sum vanishes unless $p_1 = p_2$, so that (5) reduces to $\varphi(Q)^2 N^{1/2}$. Thus

$$\min_{p \in S} |\log L(s, \chi_{pn})|^2 \leq N^{-1/2} (\log\log n)^2 + O_S(\log\log n),$$

and the theorem follows.

One lesson to be learned from this seems to be that, for delicate questions, results involving $L(1,\chi)$ are more readily obtained than those involving zeros close to $s = 1$.

REFERENCES

[1] D.R. Heath-Brown, Ternary quadratic forms and sums of three square-full numbers, *Séminaire de Théorie des Nombres de Paris* (to appear).

[2] C. Hooley, On the distribution of the roots of polynomial congruences, *Mathematika*, 11 (1964), 39-49.

[3] A.V. Malyšev, On the theory of ternary quadratic forms. IV. On the connection with the Riemann hypothesis, *Vestnik Leningrad Univ.*, 15 (1960), 14-27.

D.R. Heath-Brown
Magdalen College,
Oxford OX1 4AU

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE HARDY-LITTLEWOOD METHOD FOR EXPONENTIAL SUMS

M.N. HUXLEY and N. WATT

Recently Bombieri and Iwaniec [1, 2] introduced an analogue for exponential sums of the Hardy-Littlewood circle method for exponential integrals [8], which they applied to the Lindelöf problem of estimating the size of the Riemann zeta-function. Iwaniec and Mozzochi [6] went on to treat the divisor problem.

The first of Iwaniec and Bombieri's new ideas, the division into major and minor arcs according to the height of a rational approximation to a derivative, was also granted to Jutila, who uses it for the special exponential sums arising from explicit formulae of the Voronoi type associated with automorphic functions. In this context the rational shift in the x variable corresponds to the twisting process for producing auto-

morphic functions on a congruence subgroup.

The second idea is to use the Large Sieve to estimate the mean square size of minor arc contributions. This is only useful in contexts where the major arc sums are expected to be small (another example occurs in [4]).

The present authors have generalised the exponential sum estimate in [1] to show that $(9/56 + \varepsilon, 37/56 + \varepsilon)$ is an exponent pair for any $\varepsilon > 0$. The proof will appear as [5] and [9]. In this paper we sketch the new method, proving one of our earlier results which is much easier to obtain, but not completely superseded by the exponent pair of [5], as the result requires weaker differentiability conditions.

THEOREM. Let $f(x)$ be a real function whose second, third and fourth derivatives are continuous and nonzero for $1 \le x \le 2$. Let T be large, let M be a positive integer $\le T$. Then for any $\varepsilon > 0$

$$\sum_{m=M}^{2M-1} e(T\,F(\tfrac{m}{M})) \ll M^{\frac{27}{52}}\, T^{\frac{2}{13}+\varepsilon} + M^{\frac{1}{6}}\, T^{\frac{5}{16}+\varepsilon}$$

where the implied constant depends on ε and on the function F.

The Theorem implies that $(2/13 + \varepsilon, 35/52 + \varepsilon)$ is an exponent pair, a result out of reach by the van der Corput iteration (see [3]). The van der Corput method requires more non-vanishing conditions on the derivatives of F, both individually and in combination. These conditions ensure that neither F, nor any function derived from it by Poisson summation and Weyl differencing steps, should be approximable by a polynomial of small degree with integer coefficients. We thank Prof. W.G. Nowak for clarifying this point in discussion.

We present the proof in six steps. For full details of Steps 1 to 4 see [5], and for a more precise Step 5 see [9].

STEP 1 MAJOR AND MINOR ARCS.

Writing $f(x) = T\,F(x/M)$, we have

$$T/C_r M^r \le \left|f^{(r)}(x)\right| \le C_r T/M^r$$

for $M \le x \le 2M$, $r = 2, 3, 4$ with some constants C_r. We suppose

$$C_3 T \le M^3,$$

and choose and integer N with

$$1 \le N \le M/10, \quad N^2T \le 2C_3M^3, \quad N^4T \le M^4 .$$

Let R be the integer with

$$R^2NT \ge 2C_3M^3 > (R-1)^2NT.$$

Then $R^2 \ge N$ and we suppose

$$R \le N .$$

We cover [M,2M] by intervals I_k: $[M+(k-1)N, M+kN)$. We want to find a point in I_k with rational derivatives and expand f(x) in a Taylor series about this point. As x runs through I_k, $f''(x)/2$ runs through an interval J_k. We choose a rational point a/q with (a,q) = 1 in J_k. This will be the point with smallest denominator q, unless $R^2/N < q < R$ for the smallest denominator, in which case we take the point with second smallest denominator (which must be at least R). If $q \le R^2/N$ we call I_k or J_k a major arc, otherwise a minor arc. Thus $q \ge R$ on minor arcs.

Having chosen a/q, we pick the integer m in I_k for which $f''(m)/2$ is closest to a/q, and put $\mu = f'''(m)/6$, and pick a rational approximation b/s to $qf'(m)$ with

$$\left| b/s - qf'(m) \right| \le q/N, \quad s \le \max(1, N/q) .$$

We can now approximate f(m+x) by

$$g(x) = f(m) + \frac{bx}{qs} + \frac{ax^2}{q} + \mu x^3 .$$

STEP 2 GAUSS SUMS

Writing the quadratic Gauss sum as

$$G(a,b;c) = \sum_{n \bmod c} e_c(an^2 + bn) ,$$

we have

$$\sum_n e(\mu n^3 + \frac{an^2}{q} + \frac{bn}{qs}) =$$

$$= \frac{1}{qs} \sum_{k \bmod qs} G(as, b + k; qs) \sum_n e(\mu n^3 - \frac{kn}{qs}) .$$

We can simplify the Gauss sum. For example when q is odd

$$G(as, b + k; qs) = s\, e_q(-\overline{4a}\, d^2)\, G(a,0;q)$$

if d = (b+k)/s is an integer; otherwise the Gauss sum is zero. Thus

$$\left|\sum_n e(g(n))\right| = \frac{1}{\sqrt{q}} \left| \sum_{d \bmod q} e_q(-\overline{4a}\, d^2) \sum_n e\left(\mu n^3 - n\left(\frac{d}{q} - \frac{b}{qs}\right)\right)\right| .$$

STEP 3. POISSON SUMMATION

This process replaces the sum over d and n at the end of Step 2 by

$$\sum_h \left(\frac{q}{12h_1|\mu|}\right)^{\frac{1}{4}} e_q(-\overline{4a}\, h^2)\, e\left(-\frac{2}{\sqrt{|\mu|}}\left(\frac{h_1}{3q}\right)^{\frac{3}{2}}\right) + O((q+R)\log N)\,,$$

where h is an integer variable running through a range of length

$$\asymp |\mu| q N^3, \text{ and } h_1 = h - b/s\,.$$

On the major arcs we estimate the sum over h trivially; they give in total

$$\ll \frac{M}{\sqrt{N}} \log N + R \log N\,.$$

This estimate is very good; but if we treat all arcs as major, then we must take R = N and

$$N \asymp M\, T^{-\frac{1}{3}}\,,$$

so we only get the exponent pair (1/6, 2/3). In fact when R = N the term μn^3 in g(n) can also be removed by partial summation, and the method ends at Step 2.

STEP 4. THE LARGE SIEVE

First we tidy the sum. Writing $c = [b/s]$, $h' = h-c$ we have

$$e_q(-\overline{4a}\, h^2) = e_q(-\overline{4a}\, h'^2 + \overline{2a}\, ch' - \overline{4a}\, c^2) .$$

We use partial summation to remove the factor $(q/12h_1\,|\mu|)^{1/4}$, to replace the range of summation for h' by a bounded number of ranges of the form $[H,2H)$, where H is a power of two, and to expand the $h_1^{3/2}$ inside the exponential in powers of $\delta = h' - h_1$ and then truncate the expansion. If we now write h for h', the result is

$$\sum_n e(g(n)) \ll \frac{R}{\sqrt{q}} \sum_H \int_{-1/2}^{1/2} L(\eta) \left| \sum_{h=H}^{2H-1} e(-\underset{\sim}{x}^{(h)} \cdot \underset{\sim}{y}) \right| d\eta + \sqrt{q} \log N,$$

where $L(\eta)$ is a kernel function with

$$\int_{-1/2}^{1/2} L(\eta)\, d\eta \ll \log N ,$$

and the scalar product is between the vectors

$$\underset{\sim}{x}^{(h)} = (h^2,\ h,\ h^{3/2},\ h^{1/2}) ,$$

$$\underset{\sim}{y} = \left(\frac{\overline{4a}}{q},\ -\frac{\overline{2a}\, c}{q} - \eta,\ \frac{2}{\sqrt{|27\mu q^3|}},\ \frac{3\delta}{\sqrt{|27\mu q^3|}} \right) ,$$

corresponding to the integer h and the minor arc J_k. We take together minor arcs with $Q \le q < 2Q$; call the number of these K, satisfying

$$K \ll \frac{MR^2}{NQ^2}\left(1 + \frac{NQ}{M}\right) .$$

The vectors $\underset{\sim}{x}^{(h)}$ where h runs from H to 2H-1 form a very thin set, so we have to use Hölder's inequality and combine them in bundles of four, using

$$\left|\sum_{h} e(\underset{\sim}{x}^{(h)} \cdot \underset{\sim}{y}^{(k)})\right|^4 = \sum_{\underset{\sim}{h}} e(\underset{\sim}{x}^{(h)} \cdot \underset{\sim}{y}^{(k)})$$

where $\underset{\sim}{h} = (h_1, h_2, h_3, h_4)$,

$$\underset{\sim}{x}^{(h)} = \underset{\sim}{x}^{(h_1)} + \underset{\sim}{x}^{(h_2)} - \underset{\sim}{x}^{(h_3)} - \underset{\sim}{x}^{(h_4)} .$$

The Large Sieve is used in a general form that allows the 'integer vectors' $\underset{\sim}{x}^{(h)}$ to be badly spaced as well as the 'rational vectors' $\underset{\sim}{y}^{(k)}$:

$$\left|\sum_{\underset{\sim}{h}} \sum_{k} e(\underset{\sim}{x}^{(h)} \cdot \underset{\sim}{y}^{(k)})\right|^2 \le \left(\frac{\pi}{2}\right)^{16} AB \prod_{1}^{4} (X_i Y_i + 1)$$

where

$$X_i = 2 \max_{\underset{\sim}{h}} \left|x_i^{(\underset{\sim}{h})}\right|, \quad Y_i = 2 \max_{k} \left|y_i^{(k)}\right|,$$

A is the number of coincident pairs of vectors $\underset{\sim}{x}$, coincidence being defined by

$$\left| x_i^{(h)} \underset{\sim}{} - x_i^{(h')} \underset{\sim}{} \right| < \frac{X_i}{X_i Y_i + 1} ,$$

and B is the number of coincident pairs of vectors $\underset{\sim}{y}$, coincidence being defined by

$$\left| y_i^{(k)} - y_i^{(k')} \right| < 1/X_i .$$

STEP 5. SEMICUBICAL POWERS OF INTEGERS

The vectors $\underset{\sim}{x}^{(h)}$ indexed by (h_1, h_2, k_1, k_2) and (h_3, h_4, k_3, k_4) coincide when

$$\text{(A1)} \quad h_1^2 + \ldots + h_4^2 = k_1^2 + \ldots + k_4^2,$$

$$\text{(A2)} \quad h_1 + \ldots + h_4 = k_1 + \ldots + k_4 ,$$

$$\text{(A3)} \quad h_1^{\frac{3}{2}} + \ldots + h_4^{\frac{3}{2}} = k_1^{\frac{3}{2}} + \ldots + k_4^{\frac{3}{2}} + O(\delta H^{\frac{3}{2}}),$$

$$\text{(A4)} \quad h_1^{\frac{1}{2}} + \ldots + h_4^{\frac{1}{2}} = k_1^{\frac{1}{2}} + \ldots + k_4^{\frac{1}{2}} + O(\delta H^{\frac{3}{2}}),$$

where $\delta << Q/HN$ (this is not the δ of the vectors $\underset{\sim}{y}$). We estimate the number of solutions with

$$\text{(A5)} \quad H \le h_i, k_i < 2H .$$

LEMMA 1. The number of solutions of

$$h_1^2 + h_2^2 + h_3^3 = a,$$

$$h_1 + h_2 + h_3 = b$$

is at most $6\, d(6a - 2b^2)$.

PROOF. The equations imply

$$(3h_1 + 3h_2 - 2b)^2 + 3(h_1 - h_2)^2 = 6a - 2b^2 ,$$

and the bound follows from considering factorisation in $Q(\sqrt{-3})$.

LEMMA 2. The solutions of (A1) and (A2) form families $(h_1 + t, \ldots, h_4 + t, k_1 + t, \ldots, k_4 + t)$ as t varies. The number of families that contain an integer point with all coordinates in [1, H] and have

$$\left|(k_i - h_1)(k_i - h_2)(k_i - h_3)(k_i - h_4)\right| \leq \Delta H^4$$

for each $i = 1, \ldots, 4$ is

$$\ll H^3 + \Delta H^{4+\varepsilon}$$

for any $\varepsilon > 0$.

PROOF. If $(h_1, \ldots, h_4, k_1, \ldots, k_4)$ is a solution, so is $(h_1 + t, \ldots, h_4 + t, k_1 + t, \ldots, k_4 + t)$. The

product

$$(k_i - h_1)\ldots(k_i - h_4)$$

is an invariant of the family. If all products of this type are zero, then each k_i is equal to an h_j. There are at most $24\ H^4$ integer octuplets with this property, forming $0(H^3)$ families. We count the other families as follows. If the product involving k_1 is nonzero, then $H \geq 2$ and there are $0(\Delta H^{4+\varepsilon})$ choices for the positive integers $|k_1 - h_1|, \ldots, |k_1 - h_4|$. For fixed k_1 there are $0(\Delta H^{4+\varepsilon})$ choices for $h_1, \ldots, h_4$. We now know $k_2^2 + k_3^2 + k_4^2$ and $k_2 + k_3 + k_4$, so Lemma 1 gives $0(H^{\varepsilon})$ choices for k_2, k_3 and k_4. Redefining ε, we have the result of the Lemma.

LEMMA 3. The inequalities (A1), (A2), (A3) and (A5) have

$$\ll H^{4+\varepsilon} + \delta\ H^{5+\varepsilon}$$

solutions.

PROOF. The solutions form families of the type considered in Lemma 2. We write

$$D_n(x_1,\ldots,x_4,y_1,\ldots,y_4) = x_1^n + \ldots + x_4^n - y_1^n - \ldots - y_4^n.$$

The equation

$$D_{3/2}(h_1 + t, \ldots, h_4 + t, k_1 + t, \ldots, k_4 + t) = c$$

can be written as a polynomial equation in t of degree at most 768. Hence the solutions of the inequality

$$\left|D_{3/2}(h_1 + t, \ldots, h_4 + t, k_1 + t, \ldots, k_4 + t)\right| \leq \delta H^{3/2}$$

form at most 768 intervals on the real line. Families in which each interval contains at most one integer solution contribute $O(H^{4+\varepsilon})$ by Lemma 2 to the total number of solutions. Suppose one such interval contains T + 1 consecutive integers. By the Mean Value Theorem

$$\left|\tfrac{3}{2}\, T\, D_{1/2}(h_1+t,\ldots,h_4+t,k_1+t,\ldots,k_4+t)\right| \leq 2\delta H^{3/2}$$

for some t within the interval. Write $u_i = \sqrt{(h_i + t)}$, $v_i = \sqrt{(k_i + t)}$. For $n = 1,\ldots,4$

$$u_1^{\,n} + \ldots + u_4^{\,n} = v_1^{\,n} + \ldots + v_4^{\,n} + O(\Delta H^{n/2})$$

with $\Delta = 4\delta H/3T$. Then any symmetric function of $v_1,\ldots,v_4$ (of degree d say) equals the same function of $u_1,\ldots,u_4$ to within $O(\Delta H^{d/2})$. Hence for $i = 1,\ldots,4$

$$\prod_{j=1}^{4} (v_i - u_j) = \prod_{j=1}^{4} (v_i - v_j) + O(\Delta H^2) = O(\Delta H^2) \ ,$$

$$\prod_{j=1}^{4} (k_i - h_j) \ll \Delta H^2 \prod_{j=1}^{4} (v_i + u_j) \ll \Delta H^4 .$$

By Lemma 2 there are $0(H^{3+\varepsilon} + \delta H^{5+\varepsilon} 2^{-r})$ families in which some interval of solutions has $T \geq 2^r$. Multiplying by 2^r and summing gives $0(H^{4+\varepsilon} + \delta H^{5+\varepsilon})$ solutions (when we redefine ε) from families with nontrivial intervals of solutions.

STEP 6. POINTS INDEXED BY THE MINOR ARCS

Points $\underset{\sim}{y}$ coincide if

(B1) $\left\| \overline{4a}/q - \overline{4a}_1/q_1 \right\| \ll 1/H^2$,

(B2) $\left\| \overline{2a}\, c/q - \overline{2a}_1 c_1/q_1 \right\| \ll 1/H$,

(B3) $\mu_1 q_1^{\,3}/\mu q^3 = 1 + 0(R^2/N^2)$

(B4) $\left\| b/s - b_1/s_1 \right\| \ll Q/N$.

Let B_o be the number of coincidences with $q = q_1$. An argument using Cauchy's inequality shows that $B \ll QB_o$. Equivalently we could divide into cases according to the value of q before applying the Large Sieve.

When $q = q_1$ (B3) gives

$$\mu_1/\mu = 1 + 0(R^2/N^2) .$$

By the lower bound for the fourth derivative

$$m_1 - m \ll MR^2/N^2 ,$$

and by the upper bound for the third derivative

$$a_1 - a \ll |a|R^2/N^2 .$$

Dividing the range for 4a into a finite number of ranges $[A,2A)$ where

$$A \asymp MQ/NR^2 ,$$

we estimate B_o using the next lemma. We are unable to make use of the conditions (B2) and (B4) which involve Diophantine approximation to the first derivative $f'(m)$.

LEMMA 4. The number of pairs of rationals r/q, r_1/q with

$$A \le r, r_1 < 2A, Q \le q < 2Q ,$$

$$\|\bar{r}/q - \bar{r}_1/q\| \le \Delta_1 ,$$

$$|r - r_1| \le \Delta_2 A$$

is at most

$$AQ + 2\Delta_2 A^2 + O(\Delta_1\Delta_2 A^{2+\varepsilon} Q^{2+\varepsilon})$$

for any $\varepsilon > 0$, the O-constant depending on ε.

PROOF. Let $u = r_1 - r$, and define s by

$$|s| \le \Delta_1 q, \ \bar{r} - \bar{r}_1 \equiv s \pmod{q}.$$

Then we have

$$u = r_1 - r \equiv r r_1 s \pmod{q}.$$

CASE 1. If $u = 0$, then $s = 0$. There are $\le AQ$ such trivial solutions.

CASE 2. If $u \neq 0$, but $s = 0$, then $q \mid u$. There are Q choices for q, at most A choices for r, and

$$1 \le |u|/q \le \Delta_2 A/Q,$$

so there are at most $2\Delta_2 A^2$ solutions in this case.

CASE 3. Solutions with $u \neq 0$, $s \neq 0$. After interchanging r_1 and r if need be, we suppose $s > 0$. Then

$$r(r+u)s - u = r r_1 s - u \ge r r_1 - (A-1) \ge A^2 - A + 1 \ge 1 .$$

Hence q must be one of the $\ll (AQ)^{\varepsilon}$ factors of $r(r+u)s-u$. There are A choices for r, $\le 2\Delta_1 Q$ choices for s and as in case 2 there are $\le 2\Delta_2 A$ nonzero choices for $|u|$. Multiplying these numbers gives the third term in the upper bound.

COMPLETION OF THE PROOF

By Step 5 with

$$\delta \ll Q/HN$$

we have

$$A \ll H^{4+\varepsilon}(1 + Q/N) .$$

In Step 6 we use Lemma 4 with

$$\Delta_1 \ll \frac{1}{H^2} \ll \frac{R^4}{N^2Q^2} , \quad \Delta_2 \ll \frac{R^2}{N^2}$$

so that

$$B_o \ll A^{1+\varepsilon} Q^{1+\varepsilon}(1 + \Delta_2 A/Q + \Delta_1\Delta_2 A)$$

$$\frac{M^{1+\varepsilon} Q^2}{NR^2} \left(1 + \frac{M}{N^3} + \frac{MR^4}{N^5Q}\right) .$$

First we choose

$$N^5 \asymp MR^3, \quad N \asymp M^{11/13} T^{-3/13}, \quad R \asymp M^{14/13} T^{-5/13} .$$

These choices are valid for $T^{7/17} \le M \le T^{2/3}$. Then

$$B \ll Q B_o \ll \frac{M^{2+\varepsilon} R^2Q^2}{N^6} \left(1 + \frac{T^{9/13}}{M^{20/13}}\right) ,$$

leading to an estimate for the original sum of the Theorem

$$\ll M^{1+\varepsilon} (NR)^{-1/4} \ll M^{27/52} T^{2/13+\varepsilon}$$

for $M \gg T^{9/20}$.

For $M \ll T^{9/20}$ we choose

$$N \asymp M^{1/3}, \quad R \asymp M^{4/3} T^{-1/2} ;$$

these choices are valid for $M \gg T^{3/7}$ and give

$$B \ll \frac{M^{1+\varepsilon} Q^3}{NR^2} \left(1 + \frac{M^{10/3}}{T^{3/2}}\right),$$

which leads to the estimate

$$M^{1/6} T^{5/16+\varepsilon}$$

for the sum of the Theorem. This establishes the Theorem for $T^{3/7} \le M \le T^{2/3}$. For $M \ge T^{2/3}$ the bound

$$M^{1/2} T^{1/6+\varepsilon}$$

obtained by making all arcs major and stopping at Step 2 or Step 3 is better. This argument does not use the fourth derivative, so we can precede it with a Weyl differencing step (Lemma A of [3]) which effectively replaces f by f′ to get the estimate

$$M^{5/7} T^{1/14+\varepsilon},$$

which supplies the range $M \leq T^{3/7}$. Of course sharper versions of these two estimates can be obtained from the van der Corput theory.

To show that $(2/13 + \varepsilon, 35/52 + \varepsilon)$ is an exponent pair, we can now assume that F satisfies suitable differentiability conditions for the exponent pair $(1/9, 13/18)$ to apply. Since

$$M^{11/18} T^{1/9} \ll M^{27/52} T^{2/13+\varepsilon}$$

for $M \ll T^{9/20}$, the second term in the bound of the Theorem is needed no longer.

REFERENCES

[1] E. BOMBIERI, H. IWANIEC, On the order of $\zeta(1/2 + it)$, *Annali Scuola Normale di Pisa*, 13 (1986), 449-472.

[2] E. BOMBIERI, H. IWANIEC, Some mean value theorems for exponential sums, *Annale Scuola Normale di Pisa*, 13 (1986), 473-486.

[3] S.W. GRAHAM, An algorithm for computing optimal exponent pairs, *J. London Math. Soc.*, (2) 33 (1986), 203-218.

[4] M.N. HUXLEY, Small differences between consecutive primes II, *Mathematika* 24 (1977), 142-152.

[5] M.N. HUXLEY, N. WATT, Exponential sums and the Riemann zeta function, to appear.

[6] H. IWANIEC, J. MOZZOCHI, On the divisor and circle problems, to appear.

[7] M. JUTILA, A Method in the Theory of Exponential Sums, Tata, Bombay, to appear.

[8] R.C. VAUGHAN, The Hardy-Littlewood Method, Cambridge 1981.

[9] N. WATT, A problem on semicubical powers, to appear.

M.N. HUXLEY and N. WATT
Pure Maths. Dept. University College
Cardiff CF1 1X4
U K

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

LIMIT LAWS AND MOMENTS OF ADDITIVE FUNCTIONS IN SHORT INTERVALS

INDLEKOFER K.-H.

1. INTRODUCTION

Recently [6] we investigated the distribution of real-valued additive functions f in short intervals. For $1 \leq y \leq x$ let

$$\nu_{x,y}(n: f(n)-\alpha(x,y) \leq z\beta(x)) := $$

$$= y^{-1} \#\{n: x-y<n\leq x, f(n)-\alpha(x,y) \leq z\beta(x)\}.$$

In the above mentioned paper we proved the following short interval analogues of the Erdös-Winter theorem and a result of Kubilius, respectively.

THEOREM 1. ([6], Corollary 1). *Let* $f: \mathbb{N} \to \mathbb{R}$ *be*

additive, and let $y \geq x^{1-\delta(x)}$ *with* $\delta(x)>0$ *and* $\lim_{x\to\infty} \delta(x)=0$. *Then the frequencies* $\nu_{x,y}(n: f(n)\leq z)$ *possess a limiting distribution* $F(z)$ *if and only if the frequencies* $\nu_{x,x}(n: f(n) \leq z)$ *possess the limiting distribution* $F(z)$.

For positive y define the functions

$$A(y) := \sum_{p\leq y} \frac{f(p)}{p},$$

$$B^2(y) := \sum_{p\leq y} \frac{f^2(p)}{p}.$$

Following Kubilius, we say that a strongly additive function $f:\mathbb{N}\to\mathbb{R}$ belongs to the class H if there exists a function $r(x)$, so that, as $x\to\infty$,

$$\frac{\log r(x)}{\log x} \to 0, \quad \frac{B(r(x))}{B(x)} \to 1, \quad B(x) \to \infty.$$

For such functions we have

THEOREM 2. ([6], Theorem 4). *Let* $f\in H$ *be strongly additive, and define* y *as in theorem 1. Then the distribution functions* $\nu_{x,y}(n: f(n)-A(y)\leq zB(y))$ *possess a limit law* $F(z)$ *if and only if the distribution functions* $\nu_{x,x}(n: f(n)-A(x)\leq zB(x))$ *possess the limit law* $F(z)$.

To prove these theorems, we used sieve methods and ideas (Lemma 3) similar to those given in [5]. The same result

as in Theorem 1 (under the additional assumption $y=o(x)$) has been proved by Hildebrand ([4], Corollary 7) in his paper on multiplicative functions in short intervals. We shall use the main result from this paper of Hildebrand in combination with methods of [5] and [6] to derive the following short interval analogues of theorems of Elliott, Levin and Timofeev (see [1], Theorem 16.1 and 16.2).

THEOREM 3. *Let* $\beta: \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ *satisfy* $\beta(x) \to \infty$ *as* $x \to \infty$ *and*

$$\lim_{x\to\infty} \frac{\beta(x^u)}{\beta(x)} = 1 \qquad \text{for every } u>0.$$

If $y=y(x)$ *and* f *are defined as in Theorem 1 the following holds. In order that for some function* $\alpha(x,y)$ *the frequencies*

$$(1) \qquad \nu_{x,y}(n: f(n)-\alpha(x,y) \le z\beta(x))$$

possess a limiting distrbiution $F_1(z)$ *as* $x \to \infty$, *it is both necessary and sufficient that the frequencies*

$$(2) \qquad \nu_{x,x}(n: f(n)-\alpha(x) \le z\beta(x))$$

possess a limiting distribution $F_2(z)$ *for some function* $\alpha(x)$. *If the limit laws exist one may choose* $\alpha(x,y)=\alpha(x)$, *and* $F_1(z)=F_2(z)$.

REMARK. For the proofs of Theorem 1 and Theorem 2 we determine the asymptotic behaviour of the distribution functions of the corresponding frequencies $\nu_{x,y}(n:\ldots)$, and from this we derive necessary and sufficient conditions for the existence of the limit laws. In the proof of Theorem 3 we only compare the characteristic functions of $\nu_{x,y}(n:\ldots)$ and $\nu_{x,x}(n:\ldots)$, respectively, and obtain the desired result.

COROLLARY 1. *Let* f, $\beta(x)$ *and* $y=y(x)$ *the same as in Theorem 3. In order that the frequencies* (1) *possess the weak limiting distribution* $F(z)$,

$$(3) \qquad \nu_{x,y}(n: f(n)-\alpha(x,y) \leq z\beta(x)) \to F(z) \quad (x\to\infty),$$

it is both necessary and sufficient that there exists a constant A *so that the independent random variables* X_p (p *prime*) *which are defined by*

$$X_p = \begin{cases} f(p)-A\log p & \text{with probability } \frac{1}{p} \\ 0 & \text{with probability } 1-\frac{1}{p} \end{cases}$$

satisfy

$$(4) \qquad P\Big(\sum_{p\leq x} X_p - \omega(x) \leq z\beta(x)\Big) \to F(z) \quad (x\to\infty)$$

with a suitable $\omega(x)$.

If (3) *and* (4) *hold, one may choose* $\omega(x)=\alpha(x,y)-A\log x$. In the last part of the paper we investigate moments of strongly additive functions f. For this we define a strongly additive function f^+ by

$$(5)\qquad f^+(p) = \begin{cases} f(p) & \text{if } |f(p)| \leq B(x) \\ |f(p)| & \text{otherwise,} \end{cases}$$

and put $A^+(y) := \sum_{p\leq y} f^+(p)/p$. Then we prove

THEOREM 4. *Let* $f:\mathbb{N}\to\mathbb{R}$ *be strongly additive, and let* $y \geq x^{\varepsilon}$ $(\varepsilon>0)$. *In order that for all* $k\in\mathbb{N}$ *the inequalities*

$$\overline{\lim_{y\to\infty}} \frac{1}{B^k(y)} \sum_{\substack{p\leq y \\ |f(p)|>B(y)}} \frac{|f(p)|^k}{p} < \infty$$

(6)

$$\overline{\lim_{y\to\infty}}\ y^{-1}\ \frac{1}{B^k(y)} \sum_{m<x/y} \sum_{(x-y)/m<p\leq x/m} |f(p)|^k < \infty$$

hold, it is both necessary and sufficient that

$$(7)\qquad \overline{\lim_{y\to\infty}}\ y^{-1} \sum_{x-y<n\leq x} \left|\frac{f^+(n)-A^+(y)}{B(y)}\right|^k < \infty$$

is valid for all $k\in\mathbb{N}$.

REMARK. The proof of Theorem 4 shows that from condition (7) the inequality

$$\overline{\lim_{y\to\infty}}\ y^{-1} \sum_{x-y<n\le x} \left|\frac{f(n)-A(y)}{B(y)}\right|^k < \infty$$

follows. Furthermore, the assumption

$$\max_{p\le y} |f(p)| << B(y)$$

implies the inequalities (6) for all $k \in \mathbb{N}$.

COROLLARY 2. *Let* $f \in H$ *be strongly additive, and let* $y \ge x^{\varepsilon}$ $(\varepsilon>0)$. *If the distribution functions* $\nu_{x,y}(n: f(n)-A(y) \le zB(y))$ *possess a limit law* $F(z)$, *and if (6) holds for each* $k \in \mathbb{N}$, *then all the moments*

$$\lim_{y\to\infty} y^{-1} \sum_{x-y<n\le x} \left\{\frac{f(n)-A(y)}{b(y)}\right\}^k =: M_k$$

exist and are finite for all $k \in \mathbb{N}$. *Moreover,*

$$M_k = \int_{-\infty}^{\infty} z^k \, dF(z) \quad (k \in \mathbb{N})$$

holds for all $k \in \mathbb{N}$.

Notations.

For each $n \in \mathbb{N}$, $p(n)$ and $q(n)$ denote the smallest and largest prime divisor of n, respectively.

If $g:\mathbb{N}\to\mathbb{C}$ is an arithmetical function, then

$$M(g,x) := \sum_{n\le x} g(n) \quad \text{and} \quad g_a(n) := g(n)n^{ia} \text{ for } a \in \mathbb{R}.$$

2. SOME LEMMATA.

LEMMA 1. (Halász [3]). *Uniformly for all multiplicative functions* f *of modulus* ≤ 1 *and all* $x,T\ge 2$ *we have*

$$\frac{1}{x}M(g,x) \ll \exp\Big(-\frac{1}{4}\min_{|t|\le T} \operatorname{Re}\Big(\sum_{p\le x} \frac{1-g(p)p^{-it}}{p}\Big)\Big) + T^{-1/4}.$$

LEMMA 2. (Hildebrand [4]). *Let* f *be a multiplicative function of modulus* ≤ 1 *and* $x,y\ge 3$. *Then we have*

$$M(g,x)-M(g,x-y) = \frac{M(g_a,x)}{x}\int_{x-y}^{x} t^{-ia}dt + O(y\,R(x,y)),$$

where a is any real number satisfying

$$|a| \le x, \quad |M(g_a,x)| = \max_{|a'|\le} |M(g_{a'},x)|,$$

and

$$R(x,y) = \Big(\log \frac{2\log x}{\log(2x/y)}\Big)^{-\frac{1}{4}}.$$

LEMMA 3. *Uniformly for all multiplicative functions* g *satisfying* $0 \le g(p^m) \le c$ *for all prime powers* p^m, *the following assertions hold.*

(i) *The estimate*

$$M(g,x) - M(g,x-y) \underset{\varepsilon}{\ll} y \exp\Big(\sum_{p\le y} \frac{g(p)-1}{p}\Big)$$

is valid for $3 \le x^{\varepsilon} \le y \le x$, *where* ε *is any fixed positive number.*

(ii) *Let* $\delta(x)$ *satisfy*

$$\delta(x) > 0, \qquad \lim \delta(x) = 0,$$

and assume $g(p^m) = 1$ *for* $x^{\delta(x)} < p \le x$. *If* $\varepsilon(x) \to 0$ *such that*

$$\frac{\varepsilon(x)}{\delta(x)} \to \infty \qquad x \to \infty,$$

then we have for $x^{\varepsilon(x)} \le y \le x$

$$M(g,x) - M(g,x-y) = y \prod_{p\le y} \Big(1-\frac{1}{p}\Big)\Big(1+\sum_{m=1}^{\infty} \frac{g(p^m)}{p^m}\Big) + o(y) \quad (x\to\infty).$$

The proof of Lemma 3 is implicit in [6] , §4.

LEMMA 4. (Ruzsa [8]). *Let* $[-1,1] \to \mathbb{C}$ *be bounded, and suppose that the inequaltiy*

$$|h(t_1+t_2) - h(t_1) - h(t_2)| \le K$$

holds for all $t_1, t_2 \in [-1,1]$, *such that* $t_1+t_2 \in [-1,1]$. *Then, for all* $t \in [-1,1]$,

$$|h(t) - h(1)t| \le 3K.$$

3. PROOF OF THEOREM 3.

Let us consider the characteristic function

$$\psi_{x,y}(t) = y^{-1} \sum_{x-y<n\leq x} \exp\left(it\frac{f(n)}{\beta(x)}\right) \exp\left(it\,\frac{\alpha(x,y)}{\beta(x)}\right). \tag{8}$$

Then the frequencies $\nu_{x,y}(n: f(n)-\alpha(x,y)\leq z\beta(x))$ possess a limit law if and only if the limit

$$\psi(t) = \lim_{x\to\infty} \psi_{x,y}(t)$$

exists for all t and is continuous at t = 0. Therefore, we may assume that, with some $\tau>0$, the inequalities

$$\liminf_{x\to\infty} |\psi_{x,y}(t)| \geq c > 0.$$

hold for all $|t| \leq \tau$.

By Lemma 2 we obtain, with some $|a| \leq x$,

$$\left|\frac{1}{x} \sum_{n\leq x} e^{it\frac{f(n)}{\beta(x)}} n^{-ia}\right| \geq c'>0 \tag{9}$$

for all $|t|\leq\tau$ and for all sufficiently large x, where a may depend on x and t. We shall prove

$$\psi_{x,y}(t)=y^{-1}\sum_{x-y<n\leq x}\exp\left(it\frac{f(n)-A\log n}{\beta(x)}\right)\exp\left(-it\frac{\alpha(x,y)-A\log x}{\beta(x)}\right)+$$

$$+o(1)$$

(10)

$$=\prod_{p\leq x}(1-p^{-1})\left(1+\sum_{m=1}^{\infty}p^{-m}e^{it\frac{f(p^m)-A\log p^m}{\beta(x)}}\right)e^{it\frac{\alpha(x,y)-A\log x}{\beta(x)}}$$

$$+o(1).$$

In the first step we make use of some estimates of the ζ-function (cf. Hildebrand [4], §6).

Lemma 1 yields, uniformly in $|t|\leq\tau$, the upper bound $(x\geq 3)$

$$(11)\quad \left|\sum_{n\leq x}e^{it\frac{f(n)}{\beta(x)}}n^{-ia}\right|\ll x\exp\left(-\frac{1}{4}\mathrm{Re}\sum_{p\leq x}\frac{1-e^{it\frac{f(p)}{\beta(x)}}e^{ih(x,t)\log p}}{p}\right)$$

$$+x(\log x)^{-\frac{1}{4}}$$

for suitable numbers $h(x,t)$, satisfying

$$|h(x,t)-a|\leq\log x,$$

and hence

$$|h(x,t)|\leq|a|+\log x\leq x+\log x\quad(x\geq 3).$$

(9) and (11) imply

$$\mathrm{Re} \sum_{p \leq x} \frac{1 - e^{it\frac{f(p)}{\beta(x)}} p^{ih(x,t)}}{p} \ll 1.$$

By means if the inequalities (see [4], §6)

$$\mathrm{Re}\ (1 - \frac{z_1}{z_2}) = \frac{1}{2} \left|1 - \frac{z_1}{z_2}\right|^2 \leqq |1-z_1|^2 + |1-z_2|^2$$

(12)

$$\leqq 2\ \{\mathrm{Re}(1-z_1) + \mathrm{Re}(1-z_2)\}\ (|z_1| = |z_2| \leqq 1)$$

we deduce

$$(13) \quad \mathrm{Re} \sum_{p \leq x} \frac{1 - p^{i(h(x,t_1+t_2)-h(x,t_1)-h(x,t_2))}}{p} \ll 1$$

for $x \geqq 3$, $|t_1|$, $|t_2|$, $|t_1+t_2| \leqq \tau$. (13) may be written as

$(\delta := 1 + (\log x)^{-1})$

$$\log \left| \frac{\zeta(\delta)}{\zeta(\delta + i(h(x,t_1+t_2)-h(x,t_1)-h(x,t_2)))} \right| \ll 1.$$

Using the well-known estimate

$$\zeta(\sigma+it) = \begin{cases} \frac{1}{\sigma - 1 + it} + 0(1) & (\sigma \geqslant 1, |t| \leqq 2) \\ 0((\log|t|)^{2/3} & (\sigma > 1, |t| > 2), \end{cases}$$

we obtain

$$h(x,t_1+t_2) = h(x,t_1) + h(x,t_2) + 0\left(\frac{1}{\log x}\right) .$$

It follows at once from Lemma 4 that, with $\tilde{h}(x,\tau) = \frac{h(x,\tau)}{\tau}$,

(14) $h(x,t) = \tilde{h}(x,\tau)t + 0\left(\frac{1}{\log x}\right)$ uniformly for $|t| \leqq \tau$.

Therefore,

$$\begin{aligned} &\operatorname{Re} \sum_{p \leqq x} \frac{1 - e^{it\frac{1}{\beta(x)}(f(p)+\beta(x)\tilde{h}(x,\tau)\log p)}}{p} \\ &= \operatorname{Re} \sum_{p \leqq x} \frac{1 - e^{it\frac{f(p)}{\beta(x)} + ih(x,t)\log p}}{p} \\ &+ \operatorname{Re} \sum_{p \leqq x} \frac{e^{it\frac{f(p)}{\beta(x)}}\{e^{ih(x,t)\log p} - e^{it\tilde{h}(x,\tau)\log p}\}}{p} \end{aligned} \tag{15}$$

$$\ll 1 \quad (|t| \leqq \tau)$$

in view of

$$\sum_{p\leq x} \frac{|e^{i(h(x,t)-t\tilde{h}(x,\tau))\log p}-1|}{p}$$

$$\leq |h(x,t)-t\tilde{h}(x,\tau)| \sum_{p\leq x} \frac{\log p}{p} \ll 1.$$

Using (15) with $t' = t\,\frac{\beta(x)}{\beta(x')}$ and applying (12) again we deduce that

$$\mathrm{Re} \sum_{p\leq x} \frac{1-e^{it(\frac{\beta(x)}{\beta(x')}\tilde{h}(x,\tau)-h(x',\tau))\log p}}{p} \ll 1.$$

for $3 \leq x \leq x' \leq x^2$. In the same way as above (see (13)) we conclude that

$$\frac{\beta(x)}{\beta(x')}\,\tilde{h}(x,\tau) = h(x',\tau) + 0\left(\frac{1}{\log x}\right)$$

amd, with $\gamma(x) = -\beta(x)\,\tilde{h}(x,\tau)$,

(16) $\quad \gamma(x) = \gamma(x') + 0\left(\frac{\beta(x)}{\log x}\right), \quad 3 \leq x \leq x' \leq x^2.$

It is easy to see (cf. [1], II, p.126), that $\beta(x) = 0((\log x)^{1/2})$, and thus

(17) $\quad \gamma(x)-\gamma(x') \ll (\log x)^{-1/2}, \quad 3 \leq x \leq x' \leq x^2$.

From this we deduce first that the limit

$$A := \lim_{n\to\infty} \gamma(3^{2^n})$$

exists, since

$$\gamma(3^{2^n}) - \gamma(3^{2^m}) \ll \sum_{\ell=m}^{n} 2^{-\ell/2}.$$

Therefore, by (17)

$$\lim_{x\to\infty} \gamma(x) = A.$$

On the other hand, the inequality $\beta(x^2) < (1+1/2)\beta(x)$ holds for $x \geq x_0$, so that

$$\frac{\beta(x^2)}{\log x^2} \leq \frac{1+1/2}{2} \frac{\beta(x)}{\log x}.$$

Hence, for all $n \geq 1$,

$$\gamma(x^{2^n}) - \gamma(x) \ll \frac{\beta(x)}{\log x} \sum_{\ell=0}^{n} (3/4)^{\ell} \ll \frac{\beta(x)}{\log x}.$$

This proves

$$\gamma(x) - A << \frac{\beta(x)}{\log x}.$$

In the same way as above we obtain

$$\text{(18)}\qquad \operatorname{Re} \sum_{p\le x} \frac{1 - e^{i\frac{t}{\beta(x)}(f(p) - A\log p)}}{p} \ll 1$$

for $|t|\le \tau$ and all sufficiently large x. (18) can be written in the form

$$\sum_{p\le x} \frac{\sin^2\left(\frac{t}{\beta(x)}(f(p) - A\log p)\right)}{p} \ll 1$$

for all $|t|\le\tau/2$. From this we derive first that, with $c = \pi/|\tau|$ and $f^*(p) = (f(p) - A \log p)/\beta(x)$,

$$\text{(19)}\qquad c^{-2} \sum_{\substack{p\le x\\ |f^*(p)\pi|\le c}} \frac{|f^*(p)|^2}{p} \ll 1.$$

This follows from the inequality $|\sin\theta|\ge 2|\theta|/\pi$ for $|\theta|\le\pi/2$. Furthermore, we have

$$\sum_{\substack{p\le x\\ |f^*(p)|>c}} \frac{1}{p} = \sum_{p\le x} \frac{1}{p} - \sum_{\substack{p\le x\\ |f^*(p)|\le c}} \frac{1}{p}.$$

This implies, since $\sin\theta/\theta\le 1$ for $\theta\in\mathbb{R}$,

$$\sum_{\substack{p\le x\\ |f^*(p)|>c}} \frac{1}{p} < \sum_{p\le x} \frac{1}{p}\left(1-\frac{\sin(\tau f^*(p))}{\tau f^*(p)}\right) + \sum_{\substack{p\le x\\ |f^*(p)|>c}} \frac{1}{|\tau f^*(p)|}\,\frac{1}{p}.$$

In the last sum we have $|\tau\, f^*(p)|^{-1} \le \pi^{-1}$, and therefore

$$(1-\pi^{-1}) \sum_{\substack{p\le x\\ |f^*(p)|>c}} \frac{1}{p} \le \sum_{p\le x} \frac{1}{p}\left(1-\frac{\sin(\tau f^*(p))}{\tau f^*(p)}\right) =$$

$$= \sum_{p\le x} \frac{1}{p}\left(1-\frac{1}{2\tau}\int_{-\tau}^{\tau} \cos(tf^*(p))\,dt\right)$$

$$= \frac{1}{2\tau}\int_{-\tau}^{\tau} \mathrm{Re} \sum_{p\le x} \frac{1-e^{itf^*(p)}}{p}\,dt$$

$$\ll 1.$$

We have thus established the inequality

$$(20) \qquad \sum_{\substack{p\le x\\ |f(p)-A\log p|>u\beta(x)}} \frac{1}{p} \ll 1$$

for every positive u.

The assumptions on $\beta(x)$ imply the existence of a function $r(x)$ satisfying

$r(x) \to \infty$, $\frac{\log r(x)}{\log x} \to 0$, $\frac{\beta(x)}{\beta(w)} \to 1$ uniformly for $r(x) \leqq w \leqq x$

as $x \to \infty$.

Then there exists a function $\delta(x) \to 0$ $(x \to \infty)$ with $x^{\delta(x)} \geqq r(x)$ and a sequence $\{x_k\}$, $x_k \to \infty$, such that (see Elliott [1], II, p. 121

$$(21) \qquad \sum_{x_k^{\delta(x_k)} < p \leqq x_k} \frac{1}{p} < \delta(x_k)$$

$$|f(p) - A\log p| > 2\delta^2(x_k)\beta(x_k)$$

holds.

We now continue the proof of Theorem 3.

Let us define a multiplicative function g^* by

$$g^*(p^m) = \begin{cases} 1 & , \text{ if } x^{\varepsilon_1(x)} < p \leqq x \\ e^{it\frac{f(p^m) - A\log p^m}{\beta(x)}} & , \text{ if } p \leqq x^{\varepsilon_1(x)} \end{cases}$$

where $\varepsilon_1(x) = o(1)$ $(x \to \infty)$ will be chosen later.

Further, let $y_1 := x^{\varepsilon_1(x)}$. By Lemma 3 we obtain

$$(22) \quad y^{-1} \sum_{x-y < n \leqq x} g^*(n) = \prod_{p \leqq x^{\varepsilon_1(x)}} (1-p^{-1})\left(1 + \sum_{m=1}^{\infty} p^{-m} g^*(p^m)\right) + o(1).$$

On the other hand we have

$$\left| \sum_{x-y<n\leq x} (e^{it(f(n) - A\log n)/\beta(x)} - g^*(n) \right|$$

$$\leq \sum_{x-y<n\leq x} \left| \prod_{\substack{p^m \| n \\ y_1 < p < x}} e^{it(f(p^m) - A\log p^m)/\beta(x)} - 1 \right|$$

(23)

$$\leq \sum_{x-y<n\leq x} \left| \prod_{\substack{p^m \| n \\ p(n)\leq y \; y_1 < p}} e^{it(f(p^m) - A\log p^m)/\beta(x)} - 1 \right| +$$

$$+ 2 \sum_{\substack{x-y<n\leq x \\ \exists p>y:\, p|n}} 1$$

$$=: \Sigma_1 + 2\Sigma_2 .$$

We estimate the first sum Σ_1 by

$$\Sigma_1 \leq \sum_{\substack{x-y<n\leq x \\ p(n)\leq y}} \mu^2(n) \left| \prod_{\substack{p\|n \\ y_1<p}} e^{it\frac{f(p) - A\log p}{\beta(x)}} - 1 \right| + 2 \sum_{\substack{x-y<n\leq x \\ \exists y_1<p\leq y: p^2|n}} 1$$

(24)

$$=: \Sigma_{11} + \Sigma_{12} .$$

Define

$$P_1 := \{p: |f(p) - A\log p| > 2\delta^2(x)\ \beta(x)\}\ ,$$

$$P_2 := \{p: |f(p) - A\log p| \leq 2\delta^2(x)\ \beta(x)\}\ .$$

Then obviously

$$\Sigma_{11} < \sum_{\substack{x-y<n\leq x \\ p(n)\leq y}} \mu^2(n) \left| \prod_{\substack{p\mid n \\ p\in P_2 \\ p>y_1}} e^{it\frac{f(p)-A\log p}{\beta(x)}} - 1 \right| +$$

$$+ 2 \sum_{\substack{x-y<n\leq x \\ p(n)\leq y \\ \exists p>y_1, p\in P_1 : p\mid n}} \mu^2(n)$$

(25)

$$=: \Sigma_{11}^{(1)} + \Sigma_{11}^{(2)}\ .$$

Concerning the second sum $\sum_{11}^{(2)}$ we obtain, using (21) with $y_k = y(x_k)$,

$$(26)\quad \Sigma_{11}^{(2)} \leq y \sum_{\substack{y_1<p<y \\ p\in P_1}} \frac{1}{p} = o(y) \text{ for } y = y_k,$$

if $\varepsilon_1(x)$ satisfies $\varepsilon_1(x) \geq \delta(x)$.

The first sum in (25) may be estimated by

$$\Sigma_{11}^{(1)} \leqq |t| \sum_{\substack{x-y<n\leqq x \\ p(n)\leqq y}} \sum_{\substack{p||n \\ y_1<p \\ p\in P_2}} \left|\frac{f(p) - A\log p}{\beta(x)}\right|$$

$$<< |t| y \sum_{\substack{y_1<p\leqq y \\ p\in P_2}} \frac{1}{p} \left|\frac{f(p) - A\log p}{\beta(x)}\right|$$

(27)

$$\leqq |t| y \Big(\sum_{\substack{y_1<p\leqq y \\ p\in P_2}} \frac{1}{p} \left|\frac{f(p) - A\log p}{\beta(x)}\right|^2 \Big) \Big(\log \frac{\log y}{\log y_1}\Big)^{1/2}$$

$$<< |t| y \, \delta^2(x) \, \Big(\log \frac{1}{\varepsilon_1(x)}\Big)^{1/2}$$

$$= o(y),$$

where we used Cauchy's inequality and (19) with $c=2\delta^2(x)$ and $\delta(x)\leqq\varepsilon_1(x)$.

By means of the assumption $\log y \sim \log x$ it is straightforward to obtain the estimate

$$\Sigma_2 \leqq \sum_{m<x/y} \sum_{(x-y)/m<p\leqq x/m} 1$$

(28)

$$<< \frac{y}{\log y} (\log x - \log y) = o(y).$$

Putting these estimates together we obtain[1] (see (26))

$$\psi_{x,y}(t) = \prod_{p\leqq x} \varepsilon_1(x) (1-p^{-1}) (1+\sum_{m=1}^{\infty} p^{-m} e^{it\frac{f(p^m)-A\log p^m}{\beta(x)}}) \times$$

$$e^{it\frac{\alpha(x,y)-A\log x}{\beta(x)}}$$

(29)

$$+ O(y^{-1} \sum_{11}^{(2)}).$$

Similar estimates[1] yield (y = x), under the assumption (9),

$$\psi_{x,x}(t) = \prod_{p\leqq x} \varepsilon_1(x) (1-p^{-1}) (1+\sum_{m=1}^{\infty} p^{-m} e^{it\frac{f(p^m)-A\log p^m}{\beta(x)}}) \times$$

(30)

$$e^{it\frac{\alpha(x)-A\log x}{\beta(x)}}$$

$$+O(x^{-1} \sum_{11}^{(2)}).$$

1) For all n from the interval $(x-(1-\varepsilon)y, x]$ we have $\exp(-it(A \log n - A \log x)/\beta(x)) = 1+o(1)$ $(x\to\infty)$, while the contribution of the integers $n\varepsilon(x-y, x-(1-\varepsilon)y]$ to $\psi_{x,y}(t)$ and $\psi_{x,x}(t)$ is smaller than ε.

If the limiting distribution F(z) of (1) exists, i.e. if the characteristic function

$$\psi(t) = \lim_{x\to\infty} \psi_{x,y}(t)$$

exists, we can assert that

$$P\left(\sum_{p\leqq x_k} X_p - \alpha(x_k,y_k) \leqq z\beta(x_k)\right) \Longrightarrow F(z)$$

as $k\to\infty$. From a result of Gnedenko on the distribution laws of independent, infinitesimal random variables (see Elliott [1], I, lemma 1.31) one deduces (see [1], II, pp. 133-134) that there exists a function $\delta^*(x)\to 0 \quad (x\to\infty)$ satisfying

$$x\delta^*(x) < \sum_{p\leqq x} \frac{1}{p} < \delta^*(x)$$
$$|f^*(p)| > 2\delta^{*2}(x)$$

Then (without loss of generality we may assume that $\delta^*(x) = \delta(x)$)

$$y^{-1}\,\Sigma_{11}^{(2)} = o(1)$$

and as a consequence

$$\psi_{x,y}(t) = \prod_{p\leqq x}(1-p^{-1})\left(1+\sum_{m=1}^{\infty} p^{-m}\, e^{it\frac{f(p^m)-A\log p^m}{\beta(x)}}\right) X$$
$$e^{it\frac{\alpha(x,y)-A\log}{\beta(x)}}$$
$$+ o(1)$$

and

$$\psi_{x,y}(t) = \prod_{p \leq x} (1 - p^{-1})\left(1 + \sum_{m=1}^{\infty} p^{-m} e^{it\frac{f(p^m) - A\log p^m}{B(x)}}\right) \chi$$

$$e^{it\frac{\alpha(x) - A\log x}{B(x)}}$$

$$+ o(1).$$

From this one readily completes the proof of Theorem 3.

4. PROOF OT THEOREM 4.

We put

$$(31) \qquad \Sigma := \sum_{x-y<n\leq x} \left|\frac{f^+(n) - A^+(y)}{B}\right|^k$$

and show $\Sigma << y$, where $<<$ depends only on k.

Define

$$P_1 := \{p: |f(p)| \leq B(y)\}$$

and

$$P_2 := \{p: |f(p)| > B(y)\}.$$

Further, define two additive functions f_1 and f_2 by

$$f_i(p) = \begin{cases} f(p), & \text{if } p \in P_i \\ 0 & \text{otherwise} \end{cases}$$

and put

$$B := B(y), \qquad A := A(y),$$

$$A_i := A_i(y) = \sum_{p \le y} \frac{f_i(p)}{p}$$

for $i = 1,2$. Using the inequality $(a+b)^k \ll a^k + b^k$ $(a,b \in \mathbb{R}_o)$ $(a,b \in \mathbb{R}_o)$ we deduce

$$\Sigma \ll \sum_{x-y<n\le x} \left| \frac{f_1(n) - A_1}{B} \right|^k + \sum_{x-y<n\le x} \left| \frac{f_2(n) - A_2}{B} \right|^k \tag{32}$$

$$=: \Sigma_1 + \Sigma_2 .$$

Now, there exists $c = c(k)$ such that

$$|a|^k \ll_c |\mathrm{Re}\, a| + |\mathrm{Im}\, a| \quad \text{for } a \in \mathbb{C}.$$

Therefore, without loss of generality we may assume that f_1 is real-valued and

$$\Sigma_1 \ll \sum_{x-y<n\le x} c^{|(f_1(n) - A_1)/B|} .$$

Since $e^{|a|} \le e^a + e^{-a}$ for all $a \in \mathbb{R}$ we obtain

$$\Sigma_1 \ll \sum_{x-y<n\le x} \{c^{(f_1(n)-A_1)/B} + c^{(-f_1(n)+A_1(n))/B}\}. \tag{33}$$

Both series in (33) can be estimated by Lemma 3. Making

use of $e^a - 1 = a \log c + 0(a^2)$ for $-1 \leqq a \leqq 1$ we see that

(34) $$\Sigma_1 \ll y.$$

Bearing in mind the inequalities

$$\sum_{\substack{p \leqq y \\ p \in P_2}} \frac{1}{p} < 1$$

and

$$|A_2| \leqq \Big(\sum_{\substack{p \leqq y \\ p \in P_2}} \frac{|f_2(p)|^2}{p}\Big)^{1/2} \Big(\sum_{\substack{p \leqq y \\ p \in P_2}} \frac{1}{p}\Big)^{1/2} < B,$$

we obtain

(35) $$\Sigma_2 << \sum_{x-y<n \leqq x} \left|\frac{f_2(n)}{B}\right|^k + y =: \Sigma_2' + y.$$

To estimate the sum Σ_2' we split f_2 into the sum $f_2 = f_2^{(1)} + f_2^{(2)}$, where the strongly additive functions $f_2^{(i)}$ $(i=1,2)$ are defined by

$$f_2^{(1)}(p) = \begin{cases} f_2(p) & \text{for } p \leqq y^{1/2} \\ 0 & \text{otherwise,} \end{cases}$$

$$f_2^{(2)}(p) = \begin{cases} f_2(p) & \text{for } p \leqq y^{1/2} \\ \\ 0 & \text{otherwise.} \end{cases}$$

Then obviously

$$(36) \quad \sum_2' \ll \sum_{x-y<n\leqq x} \left\{ \left| \frac{f_2^{(1)}(n)}{B} \right|^k + \left| \frac{f_2^{(2)}(n)}{B} \right|^k \right\}.$$

We estimate the first sum in (36) by Lemma 3 and obtain

$$\sum_{x-y<n\leqq x} \left| \frac{f_2^{(1)}(n)}{B} \right|^k \ll \sum_{x-y<n\leqq x} c^{\omega_2(n)} \sum_{\substack{p\mid n \\ p\leqq y^{1/2}}} \left| \frac{f_2(p)}{B} \right|^k$$

$$(37) \quad = \sum_{p\leqq y^{1/2}} \left| \frac{f_2(p)}{B} \right|^k \sum_{\substack{x-y<n\leqq x \\ p\mid n}} c^{\omega_2(n)}$$

$$\ll y \sum_{p\leqq y^{1/2}} \left| \frac{f_2(p)}{B} \right|^k \frac{1}{p} \ll y,$$

where the strongly additive function ω_2 is defined by

$$\omega_2(p) = \begin{cases} 1 & \text{for } p \in P_2. \\ \\ 0 & \text{otherwise.} \end{cases}$$

We proceed similarly, using $\omega_2(n) = \sum_{\substack{p|n \\ y^{1/2}<p\leq x}} 1 << 1$, to

obtain for the second sum in (36)

$$\sum_{x-y<n\leq x} \left|\frac{f_2^{(2)}(n)}{B}\right|^k \ll \sum_{x-y<n\leq x} \sum_{p|n} \left|\frac{f_2^{(2)}(p)}{B}\right|^k$$

(38)

$$= y \sum_{y^{1/2}<p\leq y} \left|\frac{f_2(p)}{B}\right|^k \frac{1}{p} + \sum_{m<x/y} \sum_{(x-y)/m<p\leq x/m} \left|\frac{f_2(p)}{B}\right|^k .$$

Then (37), (38) and (35) together with (34) yield the first assertion of Theorem 4.

In the other direction, according to (34) and (35), it is enough to show

$$\sum_{x-y<n\leq x} \left|\frac{f_2^+(n)}{B}\right|^k >> y \sum_{p\leq y} \frac{1}{p} \left|\frac{f_2(p)}{B}\right|^k + \sum_{m<x/y} \sum_{(x-y)/m<p\leq x/m} \left|\frac{f_2(p)}{B}\right|^k .$$

We have

$$\sum_{x-y<n\leq x} \left|\frac{f_2^+(n)}{B}\right|^k > B^{-k} \sum_{x-y<n\leq x} \sum_{p|n} (f_2^+(p))^k$$

$$>> B^{-k} \{ y \sum_{p\leq y} \left|\frac{f_2(p)}{B}\right|^k \sum_{m<x/y} \sum_{(x-y)/m<p\leq x/m} |f_2(p)|^k \},$$

which completes the proof of Theorem 4.

REFERENCES

[1] ELLIOTT, P.D.T.A. *Probabilistic Number Theory I, II.* Springer, New York 1979, 1980.

[2] HALÁSZ, G. Ober die Mittelwerte multiplikativer zahlentheoretischer Funktionen. *Acta Math.Acad.Sci. Hung.* 19(1968), 365-403.

[3] HALÁSZ, G. On the distribution of additive arithmetical functions. *Acta Arith.* 27 (1975), 143-152.

[4] HILDEBRAND, A. Multiplicative functions in short intervals. *Can. J. Math.*

[5] INDLEKOFER, K.-H. A mean-value theorem for multiplicative functions. *Math. Z.* 172 (1980), 255-271.

[6] INDLEKOFER, K.-H. Limiting distributions of additive functions in short intervals. (Preprint 1986), *Acta Math. Acad. Sci. Hung.* ...

[7] KUBILIUS, J. Probabilistic Methods in the Theory of Numbers. *Amer. Math. Soc. Translations of Math. Monographs*, No. 11, Providence, 1964.

[8] RUZSA, I.Z. On the concertration of additive functions. *Acta Math. Acad. Sci. Hung.* 36(1980), 215-232.

INDLEKOFER K.H.

Universität-GH Paderborn
Fachbereich Mathematik-Informatik
Warburger Str. 100
D-4790 Paderborn

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE FOURTH POWER MOMENT OF THE RIEMANN ZETA-FUNCTION OVER A SHORT INTERVAL

JUTILA, M.

1. INTRODUCTION

The mean value estimate

$$(1.1) \qquad \int_{T}^{T+T^{2/3}} |\zeta(1/2+it)|^4 \, dt \ll T^{2/3+\varepsilon}$$

was proved by *H. Iwaniec* [6] as the special case $R = 1$, $T_0 = T^{2/3}$ of the following more general result: if $T \geq 2$, $T^{1/2} < T_0 \leq T$, $T \leq t_1 < t_2 < \ldots < t_R \leq 2T$, $t_{r+1} - t_r \geq T_0$, then

$$(1.2) \qquad \sum_{r=1}^{R} \int_{t_r}^{t_r+T_0} |\zeta(1/2+it)|^4 dt \ll (RT_0 + R^{1/2} T_0^{-1/2} T) T^{\varepsilon}.$$

In the proof of this, he utilized in various ways the important identities of *N. V. Kuznetsov* [9] connecting Kloosterman sums with the Fourier coefficients of Maass wave forms.

It is our object to give a new proof of (1.1) by more classical means. It suffices to prove an analogous mean value estimate for Dirichlet polynomials

$$S(M,M';t) = \sum_{M}^{M'} d(m)m^{-1/2-it},$$

namely that

$$(1.3) \qquad \int_{T}^{T+T^{2/3}} |S(M,M';t)|^2 dt \ll T^{2/3+\varepsilon}$$

for $M \asymp M'$ and $M \ll T$. Here $d(m)$ is the usual divisor function, and the notation $A \asymp B$ means that $A \ll B \ll A$. The analogous notational convention $n \sim N$ will mean that $N \leq n \leq 2N$.

Our proof of (1.3) will be based on a generalization of Voronoi's summation formula and methods developed in [8]. One of the main principles in [8] is the analogy between the divisor function $d(n)$ and the Fourier coefficients of cusp forms. Denote the nth Fourier coefficient of a cusp form of weight κ for the modular group by $a(n)$. Then the argument leading to (1.3) also shows that

$$(1.4) \qquad \int_{T}^{T+T^{2/3}} \Big| \sum_{M}^{M'} a(m) m^{-\kappa/2 \pm it} \Big|^2 dt \ll T^{2/3+\varepsilon}$$

for $M, M' \ll T$. This implies the estimate

$$\int_{T}^{T+T^{2/3}} |\varphi(\kappa/2+it)|^2 dt \ll T^{2/3+\varepsilon}$$

due to *A. Good* [3] for the cusp form L-function

$$\varphi(s) = \sum_{n=1}^{\infty} a(n) n^{-s} .$$

An interesting and crucial point in our approach is an application of a lemma of *E. Bombieri* and *H. Iwaniec* [1] concerning pairs of fractions h_1/k_1, h_2/k_2 such that $\|\bar{h}_1/k_1 - \bar{h}_2/k_2\|$ and $h_1 k_1 - h_2 k_2$ are simultaneously small. Here $\|x\|$ means the distance of x from the nearest integer, and the class $\bar{h}_i \pmod{k_i}$ is defined by $h_i \bar{h}_i \equiv 1 \pmod{k_i}$. It seems that this very result (Lemma 2 below), the proof of which is completely elementary, contains the necessary arithmetic information that enables us to dispense with "Kloostermania" in the proof of (1.3) and (1.4).

The proof of (1.3) will be given in five steps. The respective methods and results applied can be associated with the following names: 1) Gallagher, 2) Hardy-Littlewood, 3) Voronoi, 4) - 5) Bombieri-Iwaniec.

Though our present goal is to establish a mean value estimate just for the interval $[T,T+T^{2/3}]$, we shall be working with a more general interval $[T,T+T_0]$, where

$$T^{1/2+\varepsilon} \ll T_0 \ll T^{2/3} , \tag{1.5}$$

in order to make the arguments applicable in more general situations, for instance in attempts to prove (1.2) along the same lines.

ACKNOWLEDGEMENT. I am grateful to Henryk Iwaniec and Martin Huxley for kindly sending to me preprints of the fundamental papers [1] and [4]. In addition, I wish to thank Martin Huxley for showing how my original argument in section 5 could be considerably simplified by appealing to a large sieve lemma from [1].

2. FIRST STEP: GALLAGHER'S LEMMA

Consider the integral

$$I = \int_T^{T+T_0} |S(M,M';t)|^2 dt , \tag{2.1}$$

where T_0 satisfies (1.5) and $M \asymp M' \ll T$. We apply a lemma of *P. X. Gallagher* (Lemma 1.10 in [10]), according to which

$$\int_{-T}^{T} \Big| \sum_{n=1}^{\infty} a_n n^{it} \Big|^2 dt \ll T^2 \int_0^{\infty} \Big| \sum_{y}^{\tau y} a_n \Big|^2 y^{-1} dy$$

with $\tau = \exp(T^{-1})$ if the Dirichlet series $\sum a_n n^{-s}$ converges absolutely for $\sigma \geq 0$. In particular, putting $\tau = \exp(T_0^{-1})$ and letting δ be an arbitrarily small positive number (which will be fixed in the sequel), we have

$$(2.2) \qquad I \ll M^{-1} T_0^2 \int_M^{M'} \Big| \sum_{y}^{\tau y} d(n) n^{-1/2-iT} \Big|^2 dy + M^{1+\delta} T_0^{-1} .$$

Note that the range of integration (resp. summation) should actually be $[M\tau^{-1}, M']$ (resp. $[y, \tau y] \cap [M, M']$). These are simplified in (2.2) with an error which is taken into account in the second term on the right.

The length of the sum in the integrand depends on y. This minor complication can be eliminated by the following device. We replace T_0 in (2.1) by a variable u and take the average over the interval $[T_0, 2T_0]$. In the resulting averaged version of (2.2), the right hand side is a double integral in y and u. Taking y and $v = (\exp(u^{-1} - 1)y$ as the new set of variables of integration, we end up with sums of length v in the integrand. We conclude that for a certain number Y with

$$(2.3) \qquad Y \asymp MT_0^{-1}$$

we have

$$I \ll M^{-1}T_0^2 \int_M^{M'} \Big| \sum_y^{y+Y} d(n)n^{-1/2-iT} \Big|^2 dy + M^{1+\delta}T_0^{-1} \quad .$$

The integral here can be replaced by the corresponding sum with an admissible error, so finally

$$(2.4) \qquad I \ll M^{-1}T_0^2 \sum_{M\le m\le M'} \Big| \sum_{0\le n\le Y} d(m+n)(m+n)^{-1/2-iT} \Big|^2 + M^{1+\delta}T_0^{-1}$$

This implies $I \ll T_0T^{\delta}$ for $M \ll T_0$, so in the sequel we may assume that $T_0 \ll M \ll T$.

3. SECOND STEP: THE HARDY-LITTLEWOOD METHOD

To begin with, we simplify the inner sum in (2.4). The interval $[M,M']$ is split up into segments of length μ by the points $M_q = M + q\mu$ for $0 \le q \le Q$. Thus $M_0 = M$, $M_Q = M'$, and $Q \ll \mu^{-1}M$. Define further

$$(3.1) \qquad \alpha_q = \frac{T}{2\pi M_q} \quad ,$$

and write for $M_{q-1} \le m \le M_q$

$$(3.2) \qquad (m+n)^{-1/2-iT} = f(n)e(-n\alpha_q)M^{-1/2} \quad ,$$

where $e(\alpha) = e^{2\pi i\alpha}$, and

$$f(y) = e(y\alpha_q - (T/2\pi)\log(m+y))(m+y)^{-1/2}M^{1/2} .$$

A little calculation shows that $f'(y) \ll \mu M^{-2}T$ for $0 \le y \le Y$ if $\mu \gg Y$. Hence, by (2.3), we have $f'(y) \ll Y^{-1}$ if

$$\mu \asymp MT_0T^{-1} , \tag{3.3}$$

as we now suppose. Then, substituting (3.2) into (2.4), we may remove the factor $f(n)$ by partial summation to obtain

$$I \ll M^{-2}T_0^2 \sum_{q=1}^{Q} \sum_{M_{q-1}\le m\le M_q} \Big| \sum_{0\le n\le Y} d(m+n)e(-(m+n)\alpha_q)\Big|^2 + \tag{3.4}$$

$$+ M^{1+\delta}T_0^{-1},$$

where $Y \ll MT_0^{-1}$. (The meaning of Y may have been changed, but in any case its upper bound is as before).

Next we bound the right hand side of (3.4) using the following inequality, which is easy to verify: if $v(x)$ is a function satisfying $v(x) = 1$ for $M_1 \le x \le M_2 + X$ and vanishing outside a certain finite interval, then for arbitrary complex numbers a_n we have

$$\sum_{M_1\le m\le M_2} \Big| \sum_{0\le n\le X} a_{m+n}\Big|^2 \le \tag{3.5}$$

$$\le \int_0^1 \Big| \sum_m v(m)a_m e(m\alpha) \sum_{0\le n\le X} e(-n\alpha)\Big|^2 d\alpha .$$

Let $v_q(x)$ be a sufficiently many times (say J times) continuously differentiable function with support in the interval $[M_{q-1} - \mu, M_q + 2\mu]$ which satisfies

$$v_q(x) = 1 \text{ for } M_{q-1} \le x \le M_q + \mu,$$

$$v_q^{(j)}(x) \ll \mu^{-j} \text{ for } j = 0, 1, \ldots, J.$$

Such a function can be constructed, for instance, by repeated smoothing of the characteristic function of an interval, as in [8], § 2.1. Define

$$(3.6) \qquad S_q(\alpha) = \sum_m v_q(m)d(m)e(m\alpha),$$

$$U(\alpha) = \sum_0^Y e(-n\alpha) .$$

Then by (3.4) and (3.5) (with $a_m = d(m)e(-m\alpha_q)$) we have

$$I \ll M^{-2}T_0^2 \sum_{q=1}^{Q} \int_0^1 |S_q(\alpha-\alpha_q)|^2 |U(\alpha)|^2 d\alpha + M^{1+\delta}T_0^{-1} .$$

The integrand has period 1, so that α can be replaced by $\alpha + \alpha_q$. Further, since

$$U(\alpha) \ll \min(Y, \|\alpha\|^{-1}) \ll (M^{-1}T_0 + \|\alpha\|)^{-1} ,$$

we have

$$I \ll M^{-2}T_0^2 \sum_{q=1}^{Q} \int_0^1 |S_q(\alpha)|^2 (M^{-1}T_0 + \|\alpha + \alpha_q\|)^{-2} d\alpha + M^{1+\delta}T_0^{-1} .$$

At it is customary in the Hardy-Littlewood method, we dissect the interval of integration (mod 1) into Farey arcs related to a certain Farey sequence of fractions a/k in their lowest terms such that $1 \le k \le K$. The parameter K (the "order" of the sequence) will be specified later. The Farey arc about the fraction a/k is of length $\asymp (kK)^{-1}$. Put $L = \log T$. There exists a number $K_0 < K$ such that the Farey arcs A(a/k) with $k \sim K_0$ give the maximal contribution. Then

$$(3.7) \qquad I \ll LM^{-2}T_0^2 \sum_{q=1}^{Q} \sum_{k\sim K_0} \sideset{}{^*}\sum_{a \bmod k} \int_{A(a/k)} |S_q(\alpha)|^2 (M^{-1}T_0 + \|\alpha+\alpha_q\|)^{-2} d\alpha + M^{1+\delta}T_0^{-1}$$

where the sum $\sum^*$ is restricted by the condition $(a,k) = 1$.

4. THIRD STEP: A SUMMATION FORMULA OF THE VORONOI TYPE

The exponential sum $S_q(\alpha)$ for $\alpha \in A(a/k)$ is now transformed by applying the following identity which is a generalization of the classical summation formula of G. Voronoi: if $0 < a < b$ and the function f is continuously differentiable in the interval [a,b], then

$$\sum_{a\le n\le b}{}' d(n)e(na/k)f(n) =$$

$$= k^{-1}\int_a^b (\log x + 2\gamma - 2\log k)f(x)dx +$$

(4.1)

$$+ k^{-1}\sum_{n=1}^{\infty} d(n)\int_a^b f(x)\{-2\pi e(-n\bar{a}/k)Y_0(4\pi\sqrt{nx}/k) +$$

$$+ 4e(n\bar{a}/k)K_0(4\pi\sqrt{nx}/k)\}dx .$$

Here Y_0 and K_0 are Bessel functions, γ is Euler's constant, and $\sum'$ means that if a or b is an integer, then the term corresponding to n = a or n = b is to be halved. For a proof of (4.1), see [7], Theorem 4, or [8], Theorem 1.7.

In our case, $\alpha = a/k + \beta$ and $f(x) = v_q(x)e(\beta x)$, where $k \sim K_0$ and $\beta \ll (KK_0)^{-1}$. By (4.1) we have

$$S_q(\alpha) = \sum_{i=0}^{2} S_{q,i}(\alpha),$$

where

$$S_{q,0}(\alpha) = k^{-1}\int v_q(x)(\log x + 2\gamma - 2\log k)e(\beta x)dx ,$$

$$S_{q,1}(\alpha) = -2\pi k^{-1}\sum_{n=1}^{\infty} d(n)e(-n\bar{a}/k)\int v_q(x)Y_0(4\pi\sqrt{nx}/k)e(\beta x)dx,$$

$$S_{q,2}(\alpha) = 4k^{-1}\sum_{n=1}^{\infty} d(n)e(n\bar{a}/k)\int v_q(x)K_0(4\pi\sqrt{nx}/k)e(\beta x)dx.$$

Define

$$(4.2)\qquad I_i = LM^{-2}T_0^2 \sum_{q=1}^{Q} \sum_{k\sim K_0} \sideset{}{^*}\sum_{a \bmod k} \int_{A(a/k)} |S_{q,i}(\alpha)|^2 (M^{-1}T_0 + \|\alpha+\alpha_q\|)^{-2} d\alpha \ .$$

Then it follows from (3.7) that

$$(4.3)\qquad I \ll \sum_{i=0}^{2} I_i + M^{1+\delta}T_0^{-1} \ .$$

Consider first I_0. By J integrations by parts, we obtain

$$S_{q,0}(\alpha) \ll LK_0^{-1}(\mu|\beta| + 1)^{-J}\mu \ .$$

Hence $|S_{q,0}(\alpha)|$ decreases rapidly as $|\beta|$ exceeds μ^{-1}, and we have

$$I_0 \ll L^3K_0^{-2}\mu M^{-2}T_0^2 \sum_{q=1}^{Q} \sum_{k\sim K_0} \sideset{}{^*}\sum_{a \bmod k} (M^{-1}T_0 + \|a/k+\alpha_q\|)^{-2} \ .$$

The assumption $T_0 \gg T^{1/2+\varepsilon}$ is needed here to guarantee that $M^{-1}T_0 + \|\alpha+\alpha_q\|$ is of a uniform order of magnitude for $|\beta| \ll \mu^{-1+\varepsilon}$. For a given fraction a/k, there are $O(M^{-1}T)$ indices q such that $\|a/k+\alpha_q\|$ lies in a given interval of length $M^{-1}T_0$, because $\alpha_{q+1} - \alpha_q \asymp M^{-1}T_0$ by (3.1) and (3.3).

Hence

$$(4.4) \qquad I_0 \ll L^3 T_0 .$$

Turning to I_2, we suppose that $K \ll M^{1/3}$. Then, since $K_0(x)$ is an exponentially decreasing function, the term I_2 can be neglected in (4.3).

Consider finally I_1. By the well-known formula

$$(4.5) \qquad Y_0(x) \sim e^{ix} \sum_{r\geq 1} a_r x^{1/2-r} + e^{-ix} \sum_{r\geq 1} b_r x^{1/2-r}$$

(where $\sim$ now denotes an asymptotic expansion) the integrals in the definition of $S_{q,1}(\alpha)$ are essentially exponential integrals. The saddle points for the nth integral, i.e. the zeros of the functions $\pm k^{-1} n^{1/2} x^{-1/2} + \beta$, may lie in the interval of integration only if $n \ll K_0^2 \beta^2 M \ll K^{-2} M$. Thus the terms for $n > N$ with

$$(4.6) \qquad N \asymp K^{-2} M$$

involve smoothed exponential integrals without a saddle point. These integrals are small if J is taken sufficiently large and $K_0^{-1} N^{1/2} M^{-1/2} \asymp (KK_0)^{-1}$ exceeds $\mu^{-1} T^{\delta}$ (see [8], Theorem 2.3). This condition, like the assumption $K \ll M^{1/3}$, will be fulfilled if we choose

(4.7) $$K = \mu^{1/2}T^{-\delta} \asymp (MT^{-1}T_0)^{1/2}T^{-\delta}.$$

Then by (4.6)

(4.8) $$N \asymp T_0^{-1}T^{1+2\delta} .$$

The approximation error in (4.5) is negligible if sufficiently many terms are taken into account. We substitute these terms into the definition of $S_{q,1}(\alpha)$, where the series is cut at N, and use Cauchy's inequality. Then one of the resulting sums gives the maximal contribution to the right hand side of (4.2) (for i = 1). We may suppose that the maximal contribution comes from one of the leading terms, say from $a_1x^{-1/2}e^{ix}$, for otherwise the argument is similar but more trivial. Thus the interesting part of $S_{q,1}(\alpha)$ now is (up to a constant factor) the sum of O(L) sums of the type

(4.9) $$\tilde{S}_q(\alpha) = k^{-1/2} \sum_{n\sim N_0} d(n)e(-n\bar{a}/k)n^{-1/4} \times$$

$$\times \int v_q(x)x^{-1/4}e(\beta x+2\sqrt{nx}/k)dx ,$$

where $N_0 < N$. Denote by $\tilde{I}_1$ the resulting expression when $S_{q,1}(\alpha)$ is replaced by $\tilde{S}_q(\alpha)$ in (4.2) (for i = 1). Then by (4.3), (4.4), and the preceding estimations we have for a certain N_0

(4.10) $$I \ll L^2\tilde{I}_1 + L^3T_0 .$$

The rest of the proof of (1.3) will be devoted to the estimation of $\tilde{I}_1$.

We replace in $\tilde{I}_1$ the integral over $A(a/k)$ by a smoothed integral. To this end, let $w(x)$ be a smooth weight function, similar to $v_q(x)$ above. with support $[-\eta,\eta]$, where $\eta \asymp (KK_0)^{-1}$ is so large that the interval $[a/k - \eta/2, a/k + \eta/2]$ covers the arc $A(a/k)$ for each Farey fraction a/k under consideration. The integrand in the integral over $A(a/k)$ is now multiplied by $w(\alpha - a/k) = w(\beta)$, and the integral is taken over the interval $B(a/k) = [a/k - \eta, a/k + \eta]$.

To simplify the estimation of the last mentioned integral, we require that the factor $M^{-1}T_0 + \|\alpha + \alpha_q\|$ retains essentially (i.e. up to an unimportant factor T^{δ} at most) its order of magnitude in $B(a/k)$. This is the case if

$$M^{-1}T_0 \gg K^{-1}T^{-\delta} \asymp (M^{-1}T_0^{-1}T)^{1/2} .$$

Therefore we suppose that

(4.11) $$T_0^3 \gg MT .$$

This holds, in any case, for $T_0 = T^{2/3}$. There is now a nonnegative integer $\rho = \rho(q,a/k)$ such that

(4.12) $$2^{\rho}M^{-1}T_0 \ll M^{-1}T_0 + \|\alpha + \alpha_q\| \ll 2^{\rho}M^{-1}T_0T^{\delta} \text{ for } \alpha \in B(a/k) ,$$

and we have

(4.13) $$\int_{A(a/k)} |\tilde{S}_q(\alpha)|^2(M^{-1}T_0 + \|\alpha + \alpha_q\|)^{-2}d\alpha \ll$$
$$\ll 2^{-2\rho}M^2T_0^{-2} \int w(\beta)|\tilde{S}_q(\alpha)|^2d\alpha .$$

Further, replacing here $\tilde{S}_q(\alpha)$ by its definition (4.9), we obtain

(4.14) $$\tilde{I}_1 \ll LK_0^{-1} \sum_{q=1}^{Q} \sum_{k\sim K_0} \sideset{}{^*}\sum_{a \bmod k} 2^{-2\rho(q,a/k)} \iint v_q(x)v_q(y)(xy)^{-1/4} \times$$
$$\times \sum_{m,n\asymp N_0} d(m)d(n)(mn)^{-1/4} \times$$
$$\times e((n-m)\bar{a}/k)e(2(\sqrt{mx}-\sqrt{ny})/k)\lambda(x-y)dxdy ,$$

where

$$\lambda(\xi) = \int w(\beta)e(\xi\beta)d\beta .$$

Owing to the presence of the smoothing factor $w(\beta)$, the integral $\lambda(x-y)$ is negligibly small unless $|x-y| < KK_0T^{\delta}$, in which case we estimate trivially $\lambda(x-y) \ll (KK_0)^{-1}$.

Write $y = x + \xi$ in (4.14), and consider the integral over x when ξ is fixed. By the above, we may suppose that $|\xi| < KK_0T^{\delta}$. The integral is small if the function

$$e(2(\sqrt{mx} - \sqrt{n(x+\xi)})/k =$$

$$= e(2\sqrt{x}(\sqrt{m} - \sqrt{n})/k)e(-2k^{-1}\xi\sqrt{n}(\sqrt{x} + \sqrt{x+\xi})^{-1})$$

oscillates sufficiently rapidly. The second factor is rather stationary (its derivative is $\ll M^{-1}T^{\delta}$), so that the behaviour of this function depends mainly on the first factor. By repeated integration by parts (taking $\sqrt{x}$ as the new variable of integration) we find that the integral over x is small unless

$$K_0^{-1}(\sqrt{m} - \sqrt{n})/\sqrt{M} \ll \mu^{-1}T^{\delta} \asymp M^{-1}T_0^{-1}T^{1+\delta}.$$

This is equivalent to the condition $|m - n| \ll P$ with

$$P = K_0M^{-1/2}N_0^{1/2}T_0^{-1}T^{1+\delta}. \tag{4.15}$$

For simplicity, we restric ourselves in (4.14) to pairs $(q,a/k)$ for which $\rho(q,a/k) = \rho$ is fixed. If ρ is suitably chosen, then (4.14) remains true with this extra condition of summation if the factor L is replaced by L^2. As was seen above, we may assume moreover that $|x-y| < KK_0T^{\delta}$ and $|m-n| \ll P$.

5. FOURTH STEP: THE LARGE SIEVE

To estimate the right hand side of (4.14), we appeal to the following inequality due to *E. Bombieri* and *H. Iwaniec* [1].

LEMMA 1. *Let* x *and* y *be two sets of points* $\bar{x} \in R^K$ *and* $\bar{y} \in R^K$ *with components* x_k *and* y_k, *respectively, and let* $a(\bar{x})$ *for* $\bar{x} \in X$ *and* $b(\bar{y})$ *for* $\bar{y} \in Y$ *be arbitrary complex numbers. Let* $X_1, \ldots, X_K, Y_1, \ldots, Y_K$ *be positive numbers. Define*

$$A = \sum_{\substack{\bar{x},\bar{x}' \in X \\ |x_k - x_k'| \le (2Y_k)^{-1}}} |a(\bar{x})a(\bar{x}')|,$$

$$B = \sum_{\substack{\bar{y},\bar{y}' \in Y \\ |y_k - y_k'| \le (2X_k)^{-1}}} |b(\bar{y})b(\bar{y}')|,$$

$$C = \sum_{\substack{\bar{x} \in X \\ |x_k| \le X_k}} \sum_{\substack{\bar{y} \in Y \\ |y_k| \le Y_k}} a(\bar{x})b(\bar{y})e(\bar{x}\cdot\bar{y}).$$

Then

$$|C|^2 \le (2\pi^2)^K AB \prod_{k=1}^{K} (1 + X_k Y_k).$$

We write

$$2(\sqrt{mx} - \sqrt{ny})/k = \frac{2}{k}(\sqrt{m} - \sqrt{n})\sqrt{x} + \frac{2}{k}\sqrt{n}(\sqrt{x} - \sqrt{y})$$

and $y - x = \xi$, $x = M_q + u$ in (4.14). Then this inequality (with the modification made in the end of the preceding section) can be written as

$$(5.1) \qquad \tilde{I}_1 \ll L^2 K_0^{-1} 2^{-2\rho} \iint C(u,\xi)\,du\,d\xi,$$

where $C(u,\xi) = C$ is as in Lemma 1 with $K = 3$ (not to be confused with the parameter K) and

$$\bar{x} = \bar{x}^{(m,n)} = (n-m,\ \sqrt{m} - \sqrt{n},\ \sqrt{n}),$$

$$\bar{y} = \bar{y}^{(a/k,x,y)} = (\bar{a}/k,\ 2\sqrt{x}/k,\ 2(\sqrt{x} - \sqrt{y})/k),$$

$$a(\bar{x}) = d(m)d(n)(mn)^{-1/4},$$

$$b(\bar{y}) = v_q(x)v_q(y)(xy)^{-1/4}\lambda(x-y),$$

$$(X_1, X_2, X_3) = (O(N_0),\ O(P/\sqrt{N_0}),\ O(\sqrt{N_0})),$$

$$(Y_1, Y_2, Y_3) = (1,\ O(\sqrt{M}/K_0),\ O(KT^{\delta}/\sqrt{M})).$$

It is easily seen that

$$|a(\bar{x})| \ll T^{\delta}/\sqrt{N_0},$$

$$|b(\bar{y})| \ll (KK_0\sqrt{M})^{-1},$$

$$X_1Y_1 + 1 \ll N_0,$$

$$X_2Y_2 + 1 \ll K_0^{-1}P\sqrt{M/N_0} = T_0^{-1}T^{1+\delta},$$

$$X_3Y_3 + 1 \ll 1 + KT^{\delta}\sqrt{N_0/M} \ll T^{\delta}.$$

Thus, by (5.1) and Lemma 1,

$$\tilde{I}_1 \ll 2^{-2\rho_M} M^{3/2} N_0^{1/2} T_0 T^{-1+2} \max_{u,\xi} (AB)^{1/2} . \tag{5.2}$$

In the present case, the conditions in the definition of A read as follows:

$$|m_1 - n_1 - (m_2 - n_2)| < 1,$$

$$|\sqrt{m}_1 - \sqrt{n}_1 - (\sqrt{m}_2 - \sqrt{n}_2)| \ll K_0/\sqrt{M} ,$$

$$|\sqrt{n}_1 - \sqrt{n}_2| \ll \sqrt{M} T^{-\delta}/K .$$

The third condition is almost trivial, because $N_0 \ll K^{-2}M$. The first condition implies that $m_1 - n_1 = m_2 - n_2 = p$, say. Then the second condition can be written as

$$p|(\sqrt{m}_1 + \sqrt{n}_1)^{-1} - (\sqrt{m}_2 + \sqrt{n}_2)^{-1}| \ll K_0/\sqrt{M}.$$

Further, with $m_2 = m_1 + r$, this is equivalent to

$$pr \ll K_0 M^{-1/2} N_0^{3/2}.$$

Hence for fixed m_1 there are $\ll K_0 M^{-1/2} N_0^{3/2} \log N + N_0$ possibilities for m_2, n_1, and n_2 (the second term corresponds to $pr = 0$). Therefore

$$A \ll N_0^{-1} T^{2\delta} (N_0^2 + K_0 M^{-1/2} N_0^{5/2} \log N) \ll N_0 T^{3\delta}$$

Substituting this into (5.2), we obtain

$$\tilde{I}_1 \ll 2^{-2\rho_M 3/2} N_0 T_0 T^{-1+7\delta/2} B^{1/2} , \tag{5.3}$$

where B corresponds to those u and ξ giving the maximum.

6. FIFTH STEP: AN ARITHMETICAL LEMMA OF BOMBIERI AND IWANIEC

The estimation of the quantity B amounts to counting the number of quadruples $(a_1/k_1, a_2/k_2, x_1, x_2)$ such that

$$|\bar{a}_1/k_1 - \bar{a}_2/k_2| \ll N_0^{-1} , \tag{6.1}$$

$$|\sqrt{x_1}/k_1 - \sqrt{x_2}/k_2| \ll \sqrt{N_0}/P, \tag{6.2}$$

$$|(\sqrt{x_1} - \sqrt{x_1+\xi})/k_1 - (\sqrt{x_2} - \sqrt{x_2+\xi})/k_2| \ll 1/\sqrt{N_0}$$

The third condition is almost trivial and can be ignored.

Recall that $x = M_q + u$, so that the x_i are indexed according to q_i. The condition (4.12), together with (3.1), relates a_i/k_i with q_i as follows:

$$a_i/k_i + \frac{T}{2\pi M_{q_i}} = b + O(2^{\rho_M - 1} T_0 T^{\delta})$$

for a certain integer b. This can be written as

$$\frac{T}{2\pi M_{q_i}} = h_i/k_i + O(2^{\rho_M - 1} T_0 T^{\delta}) , \tag{6.3}$$

and then (6.1) implies that

$$\|\bar{h}_1/k_1 - \bar{h}_2/k_2\| \ll N_0^{-1}. \tag{6.4}$$

Henceforth we shall work with h_i/k_i instead of a_i/k_i.

Next we reformulate (6.2) in terms of the h_i/k_i. By (6.3),

$$\begin{aligned} x_i &= M_{q_i} + O(MT^{-1}T_0) \\ &= (T/2\pi)(h_i/k_i + O(2^\rho M^{-1}T_0T^\delta))^{-1} + O(MT^{-1}T_0) \\ &= (T/2\pi)(k_i/h_i) + O(2^\rho MT^{-1+\delta}T_0). \end{aligned}$$

Hence, for given h_i/k_i, there are $\ll 2^\rho T^\delta$ possibilities for q_i. When this expression for x_i is substituted into (6.2), the resulting inequality can be simplified to

$$|h_1k_1 - h_2k_2| \ll 2^\rho K_0^2 M^{-1}T_0T^\delta. \tag{6.5}$$

The relevant pairs $(h_1/k_1, h_2/k_2)$ are now determined by the conditions (6.4) and (6.5), and if the number of these is X, then

$$B \ll 2^{2\rho}(KK_0)^{-2}M^{-1}X\,T^{2\delta}. \tag{6.6}$$

The quantity X can be estimated by the following important lemma due to *E. Bombieri* and *H. Iwaniec* [1] (see also *M. N. Huxley* and *N. Watt* [4] for a generalization and a simplified proof).

LEMMA 2. *The number of pairs of rationals* $(h_1/k_1, h_2/k_2)$ *in their lowest terms satisfying* $h_i \sim H$, $k_i \sim K$ *and*

$$\|\bar{h}_1/k_1 - \bar{h}_2/k_2\| \le \Delta_1,$$

$$|h_1 k_1 - h_2 k_2| \le \Delta_2 HK$$

is

$$\ll HK + \Delta_2(H^2 + K^2) + \Delta_1(\Delta_1 + \Delta_2)H^2K^2 .$$

In our case, the numbers H and K are $\asymp K_0M^{-1}T$ and K_0. Further, $\Delta_1 \ll N_0^{-1}$ and $\Delta_2 \ll 2^{\rho}T^{-1+\delta}T_0$ by (6.4) and (6.5). Lemma 2 gives now

$$X \ll K_0^2M^{-1}T + 2^{\rho}K_0^2M^{-2}T^{1+\delta}T_0 +$$

$$+ N_0^{-1}(N_0^{-1} + 2^{\rho}T_0T^{-1+\delta})K_0^4M^{-2}T^2 .$$

Hence, by (6.6),

$$2^{-2\rho}B^{1/2} \ll (M^{-3/2}T_0^{-1/2}T + M^{-3/2}N_0^{-1}T)T^{5\delta/2}.$$

Finally, with (5.3) and (4.8), this gives

$$\tilde{I}_1 \ll (T_0 + N_0T_0^{1/2})T^{6\delta} \ll (T_0 + T_0^{-1/2}T)T^{8\delta},$$

which is $\ll T^{2/3+8\delta}$ for $T_0 = T^{2/3}$. This completes the proof of (1.3).

The above argument can be repeated for more general exponential sums depending on a parameter if Lemma 2 is

replaced by the corresponding more general lemma from [4]. We are going to return to this topic elsewhere.

REFERENCES

[1] BOMBIERI, E. and IWANIEC, H., On the order of $\zeta(1/2 + it)$, *Ann. Scuola Norm. Sup. Pisa* 13 (1986), 449-472.

[2] GALLAGHER, P. X., A large sieve density estimate near $\sigma = 1$, *Invent. Math.* 11 (1970), 329-339.

[3] GOOD, A., The square mean of Dirichlet series associated with cusp forms, *Mathematika* 29 (1982), 278-295.

[4] HUXLEY, M. N. and WATT, N., Exponential sums and the Riemann zeta function, Proc. London Math. Soc. (3) 57(1988), 1-24.

[5] IVIĆ, A., The Riemann zeta-function. John Wiley & Sons, New York 1985.

[6] IWANIEC, H., Fourier coefficients of cusp forms and the Riemann zeta-function, Séminaire de Théorie des Nombres, Univ. Bordeaux 1979/80, exposé no 18, 36 pp.

[7] JUTILA, M., On exponential sums involving the divisor function, *J. Reine Angew. Math.* 355 (1985), 173-190.

[8] JUTILA, M., Lectures on a method in the theory of exponential sums. Tata Institute of Fundamental Research, *Lectures on Mathematics and Physics* vol. 80, Bombay 1987.

[9] KUZNETSOV, N. V., Petersson's hypothesis for parabolic forms of weight zero and Linnik's hypothesis. Sums of Kloosterman sums, Mat. Sb. 111 (1980),334-383 (in Russian).

[10] MONTGOMERY, H.L., Topics in Multiplicative Number Theory, *Lecture Notes in Mathematics* 227, Springer, 1971.

M. JUTILA
Department of Mathematics
University of Turku
SF-20500 Turku 50, Finland.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

A NOTE ON THE NON-TRIVIAL ZEROS OF DIRICHLET L-FUNCTIONS

KACZOROWSKI J.

1. For a given Dirichlet character $\chi \pmod q$ let $m(\rho,\chi)$ denote the mutliplicity ot the zero of $L(s,\chi)$ at $s=\rho$. Our aim is to give some applications of k-functions, introduced by the present author in [5], to the study of $m(\rho,\chi)$. In particular we are interested in the values of linear forms of N variables at the points of the form $(m(\rho,\chi_1),\ldots,m(\rho,\chi_N))$, where $\chi_1,\ldots,\chi_N$ are non-equivalent Dirichlet characters. The importance of such type of questions was at first pointed out by S. Knapowski and P. Turán in their well-known series of papers on comparative prime number theory [8]. They were faced with the problem of non-vanishing of linear forms of type

$$(1.1)\qquad \frac{1}{\phi(q)} \sum_{\chi(\mathrm{mod}\ q)} (\overline{\chi(a)} - \overline{\chi(b)})\, m(\rho,\chi),$$

where a and b denote two residue classes (mod q), $(a,q)=(b,q)=1$, $a\not\equiv b(\mathrm{mod}\ q)$ and the summation is over all Dirichlet characters (mod q). They conjectured that the expression in (1.1) was non-zero for infinitely many non-trivial zeros of the function

$$\prod_{\chi(\mathrm{mod}\ q)} L(s,\chi).$$

This conjecture has been proved independently by I.Kátai /unpublished/ and E. Grosswald [3]. Further /quantitative/ refinements of Grosswald-Kátai's result can be found in Turán [13], Motohashi [10], A. Fujii [2] / see also §7 bellow/. For applications of this theorem in prime number theory see E. Grosswald [4], J.Kaczorowski-J.Pintz [6] , [7] and the above mentioned work of Knapowski-Turán [8].

Also the study of so called noncoincident zeros of two distinct L-functions leads to the consideration of linear forms at the points $(m(\rho,\chi_1), m(\rho,\chi_2))$. Recall, after, A. Fujii [1], that a zero ρ of $L(s,\chi_1)\, L(s,\chi_2)$ is called coincident if $m(\rho,\chi_1) = m(\rho,\chi_2)$. Otherwise, the zero is noncoincident.

2. Let us reproduce from [5] some basic facts about k-functions. For a primitive Dirichlet character χ and for every complex number z with a positive imaginary part let

$$(2.1) \qquad k(z,\chi) = \sum_{\gamma>0} e^{\rho z} ,$$

where the summation is over all non-trivial zeros $\rho=\beta+i\gamma$ of $L(s,\chi)$ with $0<\beta<1$, $\gamma>0$ and each zero apears in (2.1) according to its multiplicity. The series (2.1) is almost uniformly convergent on the upper half-plane and hence k is holomorphic there. It has analytic continuation to the meromophic function on the Riemannian surface of logarithmic type. More explicitly for $z\neq 0$ we have

$$(2.2) \quad 2\pi i k(z,\chi) = N(z,\chi) + \frac{e^{z}E_1(\frac{3}{2}z)+e^{2z}E_1(\frac{5}{2}z)+H(z,\delta)}{1-e^{2z}} +$$

$$+ h(z,\chi) ,$$

where $\delta=\delta(\chi)$ is equal to 0 or 1 so that $\chi(-1)=(-1)^{\delta}$ and N denotes the meromorphic and single-valued function defined by

$$N(z,\chi) = e^{\frac{3}{2}z} \sum_{n\geq 2} \frac{\Lambda(n)\chi(n)}{n^{3/2}((z-\log n)} + e^{-z/2} \sum_{n\geq 2} \frac{\Lambda(n)\overline{\chi(n)}}{n^{3/2}(z+\log n)} -$$

$$- \frac{1}{z} e^{-z/2} \log(q/\pi),$$

/Λ denotes the classical von-Mangoldt function/, $H(z,\delta)$ and $h(z,\chi)$ are the integral functions given by

$$H(z,0) = e^{2z} \int_{l_1} \frac{\Gamma'}{\Gamma}(w) e^{2wz}\, dw + e^{3z} \int_{3/4}^{7/4} \frac{\Gamma'}{\Gamma}(w) e^{-2wz}\, dw,$$

$$H(z,1) = e^{z} \int_{l_2} \frac{\Gamma'}{\Gamma}(w) e^{2wz} dw + e^{4z} \int_{5/4}^{9/4} \frac{\Gamma'}{\Gamma}(w) e^{-2wz}\, dw,$$

$$h(z,\chi) = \int_{l_3} \frac{L'}{L}(w,\chi)\, e^{wz}\, dw.$$

l_1, l_2 are simple and smooth curves, lying on the upper half-plane, joining -5/4 with -1/4 and -3/4 with 1/4 respectively; l_3 joins - 1/2 with 3/2, lie on the upper half-plane and has the property that there are no zeros of $L(s,\chi)$ between l_3 and real axis. E_1 is related to integral exponential function by the formula

$$E_1(z) = - Ei(-z).$$

Since $E_1(z) + \log z$ is integral we can write

$$k(z,\chi) = \frac{1}{2\pi i} \frac{e^z}{e^z - 1} \log z + N_1(Z,\chi)$$

where N is single-valued and meromorphic.

For our purposes it is enough to consider one single-valued branch of k defined on the set $\Omega = C \setminus \{iy : y \leq 0\}$. Denote by k_o this branch on Ω which on the upper half-plane is given by (2.1).

THEOREM 2.1 /see [5] theorem 2.3/ The only singularities of k_o on Ω are simple poles at the points $z=k \log p$, $k \geq 1$, p-prime, $p|q$ with residues $\frac{1}{2\pi i} \chi^k(p) \log p$ and at the points $z=-k \log p$, $k \geq 1$, p-prime, $p|q$ with residues $\frac{1}{2\pi i} \overline{\chi^k}(p) p^{-k} \log p$.

We shall also need the following

THEOREM 2.2 For $z=x+iy$, $x \geq 1$, $|y| \leq 1$, $0 < \eta < 1$ and for every primitive Dirichlet character $\chi \pmod q$, $q \geq 1$ we have

$$k(z,\chi) = \frac{e^{\frac{3}{2}z}}{2\pi i} \sum_{\substack{n=p^k \\ |k\log p - x| \leq \eta}} \frac{\Lambda(n)\chi(n)}{n^{3/2}(z-\log n)} + O(\eta^{-1} e^{\frac{3}{2}z} \log^2(2q)),$$

where the constant implied by O-notation is absolute.

PROOF. We have roughly

$$\left| \frac{e^{\frac{3}{2}z}}{2\pi i} \sum_{\substack{n=p^k \\ k\log p - x| > \eta}} \frac{\Lambda(n)\chi(n)}{n^{3/2}(z-\log n)} \right| \ll \eta^{-1} e^{\frac{3}{2}x} ,$$

$$\left| \frac{e^{-z/2}}{2\pi i} \sum_{n \geq 2} \frac{\Lambda(n)\chi(n)}{n^{3/2}(z+\log n)} \right| \ll e^{-x/2} ,$$

$$\left| \frac{\log(q/\pi)}{z\, e^{z/2}} \right| \ll \log(2q) ,$$

$$|H(z,0)| \ll e^{\frac{3}{2}x} , \quad |H(z,1)| \ll e^{\frac{3}{2}x} ,$$

$$\left| \frac{e^{z} E_1(\frac{3}{2}z) + e^{2z} E_1(\frac{5}{2}z)}{1 - e^{2z}} \right| \ll 1.$$

Let t_o denote a real number such that $0<t_o<1$ and $|L'/L(\sigma+it_o,\chi)| \ll \log^2(2q)$, for $-1/2 \leq \sigma \leq 3/2$. Such a number always exists. Applying the theorem of residues we get

$$|h(z,\chi)| \ll \left\{ \int_{-1/2}^{1/2+it_o} + \int_{-1/2+it_o}^{3/2+it_o} + \int_{3/2+it_o}^{3/2} \right\} \left| \frac{L'}{L}(s,\chi) e^{sz} \right| |ds| +$$

$$+ \sum_{0<\gamma<t_o} |e^{\rho z}| \ll \log^2(2q) e^{\frac{3}{2}x} + \sum_{0<\gamma<t_o} e^{\beta x - \gamma y}$$

$$\ll e^{\frac{3}{2}x} \log^2(2q),$$

which easily implies the required result.

3. The following notation will be standard in the rest of this paper. Let $N \geq 1$ and $q \geq 3$ denote two integers such that $N \leq \Phi(q)$ and let L be a non-zero linear form of N variables with complex coefficients,

$$L(X_1,\ldots,X_N) = \sum_{j=1}^{N} a_j X_j.$$

For a Dirichlet character $\chi \pmod q$ let $\chi' \pmod{q'}$, $q' \mid q$ denote the corresponding primitive character.

The basic theorem is following

THEOREM 3.1 Let $\chi_1,\ldots,\chi_N$ denote a sequence of N distinct Dirichlet characters (mod q). Then there exist infinitely many zeros $\rho = \beta + i\gamma$, $1/2 \leq \beta < 1, \gamma > 0$ of the function

$$(3.1) \qquad \prod_{j=1}^{N} L(s,\chi_j)$$

for which

$$(3.2) \qquad L(m(\rho,x_1),\ldots,m(\rho,\chi_N)) \neq 0.$$

Taking as a special case the linear form

$$(3.3) \quad L_1(X_1,\ldots,X_{\phi(q)}) = \frac{1}{\phi(q)} \sum_{j=1}^{\phi(q)} (\overline{\chi_j(a)} - \overline{\chi_j(b)})\, X_j$$

the above theorem implies the Grosswald-Kátai result. Taking

$$(3.4) \qquad L_2(X,Y) = X - Y$$

and two distinct L-functions, we see that theorem 3.1 implies the existance of infinitely many noncoincident zeros.

Proof of this theorem is very short. Consider the function

$$(3.5) \quad F(z) = L(k_o(z,\chi_1'),\ldots, k_o(z,\chi_N')).$$

For $z=x+iy$, $y>0$ we have

$$(3.6) \quad F(z) = \sum_{\gamma>0}{}' L(m(\rho,\chi_1),\ldots,m(\rho,\chi_N))\, e^{\rho z},$$

where the dash in (3.6) indicates that the summation is over all zeros $\rho=\beta+i\gamma$ of the function (3.1) such that $0<\beta<1$, $\gamma>0$ and each zero accurs in this sum exactly once.

F has analytic continuation to meromorphic function on Ω and, by theorem 2.1, it has simple poles at $z = k \log p$, $k \geq 1$, p- prime, $p \nmid q$ with residues

$$\frac{\log p}{2\pi i} L(\chi_1(p^k), \ldots, \chi_N(p^k)).$$

Not all of these residues are equal zero. Indeed, otherwise, by the celebrated Dirichlet prime number theorem, the sum

$$\sum_{j=1}^{N} a_j \chi_j(a)$$

would vanish for every residue class $a \pmod q$. This, however, is impossible because distinct characters are linearly independent /see. e.g. [9]/. Hence F has non-trivial singularities and thus infinitely many coefficients in (3.6) have to be non-zero. Theorem is therefore proved.

4. There is an interesting question concerning the location of the zero ρ satisfying (3.2) with possible smallest positive imaginary part.

Refinding the above considerations we get

THEOREM 4.1 There exist two absolute constants $b_o, b_1 \geq 0$ such that there is always a zero $\rho = \beta + \gamma i$ of the function (3.1) satisfying $1/2 \leq \beta < 1$, $0 < \gamma < q^{b_o}$ and

(4.1) $$|L(m(\rho,\chi_1),\ldots, m(\rho,\chi_N))| \geq q^{-b_1}||L||,$$

where $||L|| = \max_{1\leq j\leq N} |a_j|$.

The constants b_o and b_1 can be effectively computed and their values depend on the estimation of Linnik constant. It is very probable that the following conjecture is true.

CONJECTURE 1. There exists a zero $\rho=\beta + i\gamma$ of (3.1) satisfying $1/2 \leq \beta \leq 1$, $0 < \gamma < C$ and

$$|L(m(\rho,\chi_1),\ldots,m(\rho,\chi_N))|| \geq ||L||$$

with an absolute constant C.

For a fixed distinct Dirichlet characters $\chi_1,\ldots\chi_N$ (mod q) and a zero ρ define the N-dimensional vector $v(\rho)$ by the formula

$$v(\rho) = (m(\rho,\chi_1),\ldots,m(\rho,\chi_N)) \in Z^N.$$

Let V_o denote the Z-modul generated by $v(\rho)$, $0< \gamma < q^{b_o}$, $1/2 \leq \beta < 1$. Then rank $V_o = N$ since otherwise the real space $V_o \otimes R$ would be a proper subspace of R^N defined by a system of linear equations

$$L_k(X_1,\ldots,X_N) = 0$$

/L_k, k=1,2,...,K, K>0 being a non-zero linear forms/. This would contradict our theorem 4.1. Therefore we get

COROLLARY 4.1. We have $V_o \otimes R = R^N$ and rank $V_o = N$. More explicitly, there exist zeros $\rho_\ell = \beta_\ell + i\gamma_\ell$, $1/2 \leq \beta_\ell < 1, 0 < \gamma_\ell < q^{b_o}$ of the function (3.1), for which the vectors $v(\rho_\ell)$, $\ell=1,2,...,N$ form a basis of R^N.

Corollary 4.1 implies the following result which improves the lower estimate in Theorem 4.1 in case when N is "small" comparing with q.

COROLLARY 4.2. Theorem 4.1 remains true when we replace (4.1) by the following inequality

$$|L(m(\rho,\chi_1),...,m(\rho,\chi_N))| \geq ||L||\ N^{-1} \times (b_2(N-1)\log^2(2q))^{-N-1/2}$$

with an absolute $b_2>0$.

Most probably the following conjecture is also true.

CONJECTURE 2. $V_o = Z^N$.

Since rank $V_o = N$ we can at any rate conclude that the index $[Z^N : V_o]$ is finite and in fact that

$$[Z^N : V_o] \leq (b_3 N \log(2q))^N$$

with an absolute constant b_3.

5. Proof of Theorem 4.1. Let j_o denote the index such that

$$|a_{j_o}| = ||L|| = \max_{1 \leqq j \leqq N} |a_j|.$$

By orthogonality of characters

$$\frac{1}{\Phi(q)} \sum_{\substack{a \pmod q \\ (a,q)=1}} \chi_{j_o}(a)\, L(\chi_1(a),\dots,\chi_N(a)) = a_{j_o}$$

hence

$$||L|| \leqq \max_{(a,q)=1} |L(\chi_1(a),\dots,\chi_N(a))|.$$

Fix a residue class a_o, $(a_o,q) = 1$ with

$$|L(\chi_1(a_o),\dots,\chi_N(a_o))| \geqq ||L||.$$

By the celebrated Linnik's theorem /see e.g. [12]/ there exists a prime number p_o such that

$$p_o \equiv a_o \pmod q \quad \text{and} \quad p_o \leqq q^{c_o}$$

with an absolute constant c_o.

Write

$$z_o = \log p_o + \frac{i}{c_2 q^{c_1}}, \quad c_1 = 2.5c_o + 2,$$

$$\eta = \frac{\log 2}{2\, q^{c_o}} ,$$

where c_2 is sufficiently large. Since, if $p^k \neq p_o$,

$$|k \log p - \log p_o| \geq \log\left(1 + \frac{1}{p_o}\right) \geq \frac{\log 2}{p_o} > \eta ,$$

Theorem 2.2 furnishes

$$(5.1)\quad |F(z_o)| = \frac{\log p_o}{2\pi}\, c_2\, q^{c_1} |L(\chi_1(a_o), \ldots, \chi_N(a_o))| + O(\|L\| q^{c_1})$$

$$\geq \frac{\log 2}{2\pi}\, c_2\, q^{c_1} \|L\| + O(\|L\| q^{c_1})$$

$$\geq 2 \|L\| q^{c_1}$$

if only c_2 is large enough.

For $T \geq 1$ we have

$$\Big| \sum_{j=1}^{N} a_j \sum_{\gamma_j \geq T} e^{\rho z_o} \Big| \leq \|L\| N\, p_o \max_{1 \leq j \leq N} \sum_{\gamma_j \geq T} e^{-\gamma_j/(c_o q^{c_1})}$$

$$\ll \|L\|\, N\, q^{c_o + 2c_1} \sum_{\gamma_j \geq T} \frac{1}{\gamma_j^2} \ll \|L\|_q^{2c_1 + c_o + 1} \frac{1}{T} \log(qT).$$

Hence

$$(5.2)\qquad \Big| \sum_{j=1}^{N} a_j \sum_{\gamma_j \geq T} e^{\rho z_o} \Big| \leq \|L\| q^{c_1}$$

if $T = q^{c_3}$ with sufficiently large c_3.

If now $|L(m(\rho,\chi_1),\dots,m(\rho,\chi_N))| \leq M$ for all zeros $\rho=\beta+i\gamma$, $1/2\leq\beta<1$, $0<\gamma<q^{c_3}$ then

$$(5.3)\qquad \left| \sum_{0<\gamma<q^{c_3}} L(m(\rho,\chi_1),\dots,m(\rho,\chi_N))e^{\rho z_o} \right| \leq$$

$$\leq M_o \sum_{0<\gamma<q^{c_3}} 1 \leq M\, q^{c_4}.$$

Hence, gathering (5.1), (5.2) and (5.3) we get

$$2\,q^{c_1}||L|| \leq |F(z_o)| \leq M\,q^{c_4} + ||L||q^{c_1}$$

and

$$M \geq ||L||q^{c_1-c_4}.$$

Taking $b_o=c_3$ and $b_1=c_4-c_1$ we get the assertion of our theorem.

6. Proof of Corollary 4.2. By Corollary 4.1 we can choose a basis of R^N consisting of the vectors $v(\rho_l)$, $l=1,2,\dots,N$, where $\rho_l=\beta_l+i\gamma_l$ are zeros of the function (3.1) such that $1/2\leq\beta_l<1$, $0<\gamma_l<q^{c_o}$. The determinant

$$D = \det [m(\rho_l,\chi_j)]_{\substack{1\leq l\leq N\\ 1\leq j\leq N}}$$

is non-zero. Since evidently $D \in Z$ we have $|D| \geq 1$. Consider now the system of linear equations

$$L(v(\rho_l)) = A_l \quad . \quad l = 1,2,\ldots, N.$$

Crámer rule implies

$$a_j = D_j/D$$

where D_j denotes the determinant obtained from D by exchanging its j-th column by the vector $[A_1,..,A_N]^T$. Applying Laplace expansion and Hadamard inequality we get /with the obvious meaning of D_{jl}/:

$$|D_j| \leq \sum_{l=1}^{N} |A_l||D_{jl}| \leq \sum_{l=1}^{N} |A_l| \prod_{k\neq j} \sqrt{\sum_{h\neq l} m^2(\rho_k,\chi_h)}.$$

Since $m(\rho_k,\chi_h) << \log q$, hence

$$||D_j| \leq \max_{1\leq l\leq N} |A_l| \; N \; (b_2(N-1) \log^2 q)^{(N-1)/2}$$

and finally

$$|L| = |a_{j_0}| \leq |D_{j_0}| \leq \max_{1\leq l\leq N} |A_l| \; N(b_2(N-1)\log^2 q)^{(N-1)/2}$$

which ends the proof.

7. Our method leads also to some estimates from below for the number of zeros $\rho=\beta+i\gamma$, $0<\beta<1$, with $0<\gamma<T$ and $L(v(\rho))\neq 0$. Let for $T\geq 1$

$$f(T,L) = \sum_{\substack{0<\gamma<T \\ L(v(\rho))\neq 0}} 1$$

and

$$f^*(T,L) = \sum_{\substack{0<\gamma<T \\ L(v(\rho))\neq 0}} \sum_{j=1}^{N} m(\rho,\chi_j).$$

The result is as follows.

THEOREM 7.1. For T tending to infinity we have

$$f^*(T,L) \gg \frac{T}{\log\log T}, \tag{7.1}$$

$$f(T,L) \gg \frac{T}{\log T \log\log T}. \tag{7.2}$$

The problem of estimating $f(T,L)$ in the special case $L = L_1$, where L_1 is defined by (3.3) has been posed by S.Knapowski and P.Turán [8]. Turán himself proved, [13], that

$$f(T,L_1)) \gg \exp((\log T)^{1/5})$$

and under Riemann hypothesis

$$f(T,L_1) \gg T^{1/2}.$$

This was improved by Motohashi [10] to

$$f(T,L_1) \gg T^{1/10} (\log T)^{-3}.$$

A. Fujii [1],[2] developed a method which implies

(7.3) $\quad f(T, L_i) \geq A\, T \log T,\ i=1,2,$

/L_2 is defined by (3.4)/ which, up to the value of A, is the best possible estimate of this type. By a suitably adapted Fujii's method one can improve Theorem 7.1. It would be very interesting to prove a result as sharp as (7.3) by the methods of this paper or, more generally, by applying the theory of k-functions.

Proof of Theorem 7.1 is also very short. Fix a prime p_o such that the residue of the function F defined by (3.5) at the point $z = \log p_o$ is non-zero.

Then

$$|F(\log p_o + iy)| \geq \frac{A}{y}, \qquad A>0,$$

as $y \to 0^+$.

For sufficiently large T we have

$$\Big|\sum_{\gamma>T} L(v(\rho))\, e^{\rho(\log p_o+iy)}\Big| \leq \sum_{j=1}^{N} |a_j| \Big|\sum_{\gamma_j>T} e^{\rho_j(\log p_o+iy)}\Big|$$

$$\ll \sum_{n\geq T} e^{-ny} \log n.$$

choose y so that $c_5 yT = \log\log T$ with large enough absolute c_5. Then the last sum is $\leq A/(2y)$. Hence

$$f^*(T,L) >> \Big| \sum_{o<\gamma<T} L(v(\rho))\, e^{\rho(\log p_o + iy)} \Big|$$

$$>> A/(2y) \gg \frac{T}{\log \log T}$$

and (7.1) follows. Since $f^*(T,L) << \log T\, f(T,L)$, the proof of (7.2) is also complete.

8. On the upper half-plane each function $k(z,\chi)$ is given by a generalized Dirichlet series with complex exponents. A general theory of such series has some interesting applications to our problems. For instance, a theorem of Pólya [11] says that if the function f is defined by the generalized Dirichlet series of type

$$(8.1) \qquad f(z) = \sum_{k=1}^{\infty} a_k\, e^{\lambda_k z},$$

where $0 < |\lambda_1| < |\lambda_2| < \ldots, |\lambda_k| \to \infty$ denote arbitrary complex numbers such that

$$(8.2) \qquad \lim_{k \to \infty} \frac{k}{|\lambda_k|} = 0,$$

then the domain of existence of the function f is convex.

Since the function F defined by (3.5) is of the form (8.1) and its domain of existance, by Theorem 2.1,

is not convex we see that the condition (8.2) cannot be satisfied in this case. Hence we obtain

THEOREM 8.1. For T tending to infinity we have

$$f(T,L) = \Omega(T).$$

REFERENCES

1 A. FUJII, On the zeros of Dirichlet L-functions V, *Acta Arith.* 28/1975/,pp. 395-403.

2 A. FUJII, On the zeros of Dirichlet L-functions VII, *Acta Arith.* 29/1976/,pp.59-68.

3 E. GROSSWALD, Sur une propriete des racines complexes des functions L(s,), *C.R.Acad.Sci.* Paris, 260/1965/,pp.4299-4302.

4 E. GROSSWALD, Oscillation theorems of arithmetical functions, *Trans.Amer.Math.Soc.*, 126/1967/,pp.1-28.

5 J. KACZOROWSKI, The k-functions in multiplicative number theory I, On complex explicit formulae, *Acta Arith.* to appear.

6 J. KACZOROWSKI, J. PINTZ, Oscillatory properties of arithmetical functions, I, *Acta Math.* Hung. 48,1-2, /1986/, pp. 173-185.

7 J. KACZOROWSKI, J. PINTZ, Oscillatory properties of arithemtical functions, II, ibidem 49,3-4,/1987/,pp. 441-453.

8 S. KNAPOWSKI, P. TURAN, Comparative prime number theory, I, *Acta Math. Hung.* 8/1962/, pp. 299-314.

9 S. LANG, Algebra, Addison-Wesley Publ. Co. 1970.

10 Y. MOTOHASHI, On the distribution of the zeros of Dirichlet s L-functions, *Acta Arith.* 22/1972/,pp. 107-112.

11 G. PÓLYA, Eine Verallgemeinerung des Fabryschen Lückensatzes, *Nachr. Geselesch.* Wisseensch. Göttingen, 1927, pp. 187-195.

12 K. PRACHAR, Primzahlverteilung, Springer 1957.

13 P. TURÁN, On a problem concerning the zeros of Dirichlet s L-functions, *Publ. Ramanujan* Institute 1/1969/,pp.95-100,

KACZOROWSKI, J.
Institute of Mathematics,
A. Mickiewicz University,
Poznan, P o l a n d

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON NUMBER OF COSETS IN NON-NATURAL DISJOINT COVERING SYSTEMS

KOREC I.

1. INTRODUCTION AND BASIC NOTIONS

We shall deal with disjoint covering systems (DCS) of (Z, +) by residue classes and with DCS of arbitrary groups by their cosets as well. To have unique terminology, we shall use the group terms even in the results about (Z, +). For example, we shall speak about cosets and indices instead of residue classes and moduli. The results about DCS of arbitrary groups can be substantially more general than the results about DCS of integers. (Usually universal statements are stronger and existential ones are weaker.) However, the results about DCS of (finite) cyclic groups can be easily translated into the results about DCS of integers, and conversely. Indeed, the canonical morphisms of (Z, +) onto finite cyclic

groups can be used for this purpose. We shall usually leave this translation to the reader. Only the main result, Theorem 8, will be given also in number-theoretical terms:

THEOREM 1. Let $a_1 \pmod{m_1}$, ..., $a_k \pmod{m_k}$ be a non-natural DCS of integers, let $m = \ell.c.m.(m_1,\ldots,m_k)$ be its common modulus and p_3 be the third smallest prime divisor of m. Then

(1.1) $$k \geq p_3 + f(m).$$

Here (and elsewhere below) $\ell.c.m.$ denotes the least common multiple and f denotes the function defined by

(1.2) $f(p) = p-1$ and $f(mn) = f(m) + f(n)$

for every prime p and all positive integers m, n. This theorem is stronger than Theorem 4.8 of [4] in the sense that the common modulus m is used instead of a modulus m_i. On the other hand, it is weaker in the sense that $p_3 + 1$ is replaced by p_3. We state the hypothesis that p_3 can be replaced by $p_3 + 1$ in (1.1).

A (left) coset $A = aH$ of a group G by its subgroup H will be called a H-coset or simply a coset (of G); it will be called invariant in G if H is invariant in G and its index [G:A] is defined to be equal [G:H]. If $X \subseteq G$ then [X] will denote the subgroup generated by X; hence $[X^{-1}X]$ will denote the least group F such that X is

contained in a F-coset.

DEFINITION 2. Let G be a group and $X \subseteq G$. We shall say that a system $S=\{a_1G_1,\ldots, a_kG_k\}$ is a disjoint covering system (abbreviation: DCS) of X if the cosets $a_1G_1,\ldots, a_kG_k$ are pairwise disjoint and $\cup S=X$. We shall say that DCS S is invariant /in G/ if $G_1,\ldots,G_k$ are invariant subgroups of $[X^{-1}X]$ /of G, respectively/. The indices of $G_1, \ldots, G_k$ in G will be also called the indices of S in G and their least common multiple will be called the common index of S in G; if $G=[X^{-1}X]$ then "in G" would be omitted.

If the group G is cyclic then the common index of S from Definition 2 is equal to $q=[[X^{-1}X] : G_1 \cap \ldots \cap G_k]$; in general it is only a divisor of q.

DEFINITION 3. Let G be a group, $X \subseteq G$ and S, T be DCS of X. We shall say that T arises from S by splitting if $T \neq S$ and there is $A \in S$ such that $S - \{A\} \subseteq T$. We shall say that T arises from S by natural splitting if S arises from T by splitting and all elements of T - S are (left) cosets by the same subgroup of G.

A finite sequence of DCS of X

(3.1) $S_0, S_1, \ldots, S_n$

will be called a splitting sequence of T if $S_n = T$ and for every $i = 1,\ldots, n$ DCS S_i arises by splitting from

S_{i-1}. It will be called maximal if no member can be inserted in front of S_0 or between some S_{i-1}, S_i so that the resulting sequence is a splitting sequence of T.

The splitting sequence (3.1) will be called natural if $S_0 = \{X\}$ and every S_i, $i = 1, \ldots, n$, arises from S_{i-1} by natural splitting. The DCS T will be called natural if there is a natural splitting sequence for T. A splitting sequence or a DCS will be called non-natural if they are not natural.

A DCS S of X will be called irreducible if it contains at least two members and the union of no subset R of S, $1 < \mathrm{card}(R) <$ is a coset.

Notice that only DCS of cosets can be natural; otherwise the condition $S_0 = \{X\}$ cannot be fulfilled. Natural irreducible DCS of (cosets of) cyclic groups can be easily characterized: their common indices are primes. By [3] the common index of every non-natural irreducible DCS of (Z, +) has at least three prime divisors; this results can be immediately generalized to DCS of cosets of cyclic groups.

2. GENERALIZATION OF MYCIELSKI-ZNÁM'S INEQUALITY

THEOREM 4. Let G be a group, let H be a subgroup of G with finite index, let $X \subsetneq G$ be a union of several left H-cosets of G and let

(4.1) $a_1G_1, a_2G_2, \ldots, a_kG_k$

be an invariant disjoint covering of X. Then

(4.2) $k \geq 1 + f([H:H \cap G_1 \cap \ldots \cap G_k])$.

Moreover, if X is not a coset of G then

(4.3) $k \geq 2 + f([H:H \cap G_1 \cap \ldots \cap G_k])$.

PROOF. We shall write A(i) instead of a_iG_i and G(i, j) instead of $G_i \cap G_{i+1} \cap \ldots \cap G_j$. Let $H_1, \ldots, H_s$ be all H-cosets contained in X. We may assume $a_1 = e$ and $H_1 = H$. The number of $H \cap G(1, k)$-cosets contained in X is

$$n = [G_1:H \cap G(1, k)] + \ldots + [G_k:H \cap G(1, k)].$$

(We may not form the factor group $G/(H \cap G(1, k))$ because H need not be an invariant subgroup of G.) We shall prove Theorem 4 by induction with respect to n. If n=1 then k=1 and $H \subseteq G_1$, hence (4.2) obviously holds; (4.3) need not hold because X=A(1) is a coset of G. For n>1 we shall distinguish four cases.

Case I: there are $i \in \{1,\ldots,k\}$ and $j \in \{1,\ldots,s\}$ such that $A(i) \cap H_j = \emptyset$. Change (if necessary) the order in (4.1) so that for suitable integer u the cosets A(1),...,A(u) have nonempty intersection with H and the other members of (4.1) are disjoint with H. To estimate u, consider the cosets

$$H \cap A(1), \ldots, H \cap A(u)$$

and use the inductive assumption (with H instead of X).

So we obtain

$$u \geq 1 + f([H:H\cap G(1, u)]).$$

To estimate $k - u$ let us consider the set

$$Y = A(u + 1) \cup \ldots \cup A(k).$$

The set Y is a union of several $H\cap G(1, u)$-cosets, and by the inductive assumption (with Y instead of X and H $G(1, u)$ instead of H) we have

$$k - u \geq 1 + f([H\cap G(1, u):H\cap G(1, u)\cap G(u + 1, k)]) =$$

$$= 1 + f([H\cap G(1, u):H\cap G(1, k)]).$$

Together we have

$$k = u + (k - u) \geq 1 + f([H:H\cap G(1, u)]) +$$

$$+ 1 + f([H\cap G(1, u):H\cap G(1, k)]) =$$

$$= 2 + f([H:G(1, k)]),$$

and hence we have proved both (4.2) and (4.3).

Notice that if X is not a coset of G then Case I takes place; moreover, an even stronger condition holds:

For every $i\in\{1, \ldots, k\}$ there is $j\in\{1, \ldots, s\}$ such that $A(i)\cap H_j=\emptyset$,

Indeed, if for example $A(1)\cap H_j = G_1\cap H_j \neq \emptyset$ for all $j=1,\ldots,s$ then $X=G_1H$, hence X is a coset of G. So we need not prove (4.3) in further cases.

Case II: $s>1$ and $A(i)\cap H_j \neq \emptyset$ for all $i=1,\ldots,k$, $j=1, \ldots,s$. The system

$$H\cap A(1), \ldots, H\cap A(k)$$

is a disjoint covering system of H, and by the inductive assumption (with H instead of X) we have

$$k \geq 1 + f([H:H\cap(H\cap G_1)\cap\ldots\cap(H\cap G_k)]) =$$
$$= 1 + f([H:H\cap G(1, k)]),$$

i.e. (4.2).

Case III: $s = 1$ (i. e. $X = H$) and all groups $G_1, \ldots, G_k$ are maximal invariant subgroups of H ($k>1$ because $n>1$). Since $A(1), \ldots, A(k)$ are pairwise disjoint, we have $G_1 = \ldots = G_k$, hence $G_1\cap H = \ldots = G_k\cap H$ and therefore

$$k = [H:H\cap G_1] \geq 1 + f([H:H\cap G_1]) =$$
$$= 1 + f([H:H\cap G(1, k)]).$$

Case IV: $s = 1$ and for some $m\in\{1, \ldots, k\}$ the group G_m is not a maximal proper invariant subgroup of H. Let F be a maximal proper invariant subgroup of H which contains G_m, let $p = [H:F]$ and let $F_1 = F, \ldots, F_p$ be the list of F-cosets of H. If a coset $A(i)$ has nonempty intersection with at least two F-cosets then it has nonempty intersection with all F-cosets of H. Therefore we can renumber the members of (4.1) so that there are integers

$$0 \leq i_0 < i_1 < \ldots < i_p = k$$

such that for all $j = 1, \ldots, p$ and $i = 1, \ldots, k$:

a) $A(i)\subseteq F_j$ if and only if $i_{j-1} < i \leq i_j$;

b) $A(i)$ has nonempty intersection with all $F_1, \ldots, F_p$ if and only if $i \leq i_0$.

The inequalities $i_{j-1} < i_j$ are consequences of our choice

of F. We know that a coset F_j contains a coset A(i) (because $G_i \subseteq F$ for some i = 1, ..., k). Counting the numbers of $F \cap G(1, k)$-cosets in F_1, ..., F_p we can show that every F_j contains a coset A(i). The cosets

$$F \cap A(1), \ldots, F \cap A(i_0), A(i_0 + 1), \ldots, A(i_1)$$

form a disjoint covering system of F, and we can use the inductive assumption (with F instead of H) for it. So we obtain

$$i_1 \geq 1 + f([F:F \cap (F \cap G_1) \cap \ldots \cap (F \cap G(i_0)) \cap \cap G(i_0 + 1) \cap \ldots \cap G(i_1)]) =$$
$$= 1 + f([F:G(1, i_1)]).$$

For every j = 2, ..., p consider the system

$$A(i_{j-1} + 1), \ldots, A(i_j);$$

its union Y_j is nonempty, and it is a union of several $G(1, i_{j-1})$-cosets because

$$Y_j = F_j - (A(1) \cup \ldots \cup A(i_0))$$

and $G(1, i_{j-1})$ $G(1, i_1)$ F. By the inductive assumption (with $G(1, i_{j-1})$ instead of H) we obtain

$$i_j - i_{j-1} \geq 1 + f([G(1, i_{j-1}):G(1, i_{j-1}) \cap \cap G(i_{j-1} + 1, i_j)]) =$$
$$= 1 + f([G(1, i_{j-1}):G(1, i_j)]).$$

Together we have

$$k = i_1 + (i_2 - i_1) + \ldots + (i_p - i_{p-1}) \geq$$
$$\geq [1 + f([F:G(1, i_1)]) + 1 + f([G(1, i_1):G(1, i_2)]) + \ldots + 1 + f([G(1, i_{p-1}):G(1, i_p)]) =$$
$$= p + f([F:G(1, i_p)]) \geq$$

$$\geq 1 + f(p) + f([F:G(1, k)]) =$$

$$= 1 + f([H:F]) + f([F:G(1, k)]) =$$

$$= 1 + f([H:H\ G(1, k)]).$$

Hence (4.2) holds also in this case, which completes the proof of the theorem.

The Mycielski-Znám's inequality can be obtained from (4.2) if we put $X = G = H$.

3. THE INEQUALITY FOR NON-NATURAL DCS

We shall start with the case of irreducible DCS; the generalization to arbitrary DCS (of cyclic groups) will be straightforward.

THEOREM 5. Let G be a cyclic group, let

(5.1) $$a_1G_1, \ldots, a_kG_k$$

be an irreducible non-natural DCS of G, let n be the common index of (5.1) and let p be the greatest prime divisor of n. Then

(5.2) $$k \geq p + f(n).$$

PROOF. Let F be the maximal proper subgroup of G with the index p and let $F_1, \ldots, F_p$ be the list of all F-cosets of G. Permute the elements of (5.1) so that there are integers

$$0 \leq i_0 \leq i_1 \leq \ldots \leq i_p = k$$

such that for all $j = 1, \ldots, p$ and $i = 1, \ldots, k$:

a) $A(i) \subseteq F_j$ if and only if $i_{j-1} < i \leq i_j$;

b) $A(i)$ has a nonempty intersection with (at least two and hence) all cosets $F_1, \ldots, F_p$ if and only if $i \leq i_0$.

Analogously as in Case IV of the proof of Theorem 4 we can show $i_{j-1} < i_j$. Moreover, $i_0 > 0$ holds. Indeed, if $i_0 = 0$ then every member of (5.1) is a subset of some F_j, $j \in \{1, \ldots, p\}$. If (5.1) consists of $F_1, \ldots, F_p$ then it is natural, otherwise it is reducible; in both cases we have a contradiction. Therefore we have

$$0 < i_0 < i_1 < \ldots < i_p = k.$$

Further, analogously as in Case IV we can prove

$$i_1 \geq 1 + f([F:G(1, i_1)]).$$

For every $j = 2, \ldots, p$ we shall consider the DCS

$$A(i_{j-1} + 1), \ldots, A(i_j).$$

Its union Y_j is a union of several $F \cap G(1, i_{j-1})$-cosets (also a union of several $F \cap G(1, i_0)$. However, Y_j is not a coset of G because (5.1) is irreducible DCS. Therefore we can use the inequality (4.3) which gives

$$i_j - i_{j-1} \geq 2 + f([F \cap G(1, i_{j-1}) : F \cap G(1, i_{j-1}) \cap G(i_{j-1}+1, i_j)]) =$$

$$= 2 + f([G(1, i_{j-1}):G(1, i_j)]).$$

From these inequalities we obtain

$$\begin{aligned} k &= i_1 + (i_2 - i_1) + \ldots + (i_p - i_{p-1}) \geq \\ &\geq 1 + f([F:G(1, i_1)]) + 2 + f([G(1,i_1):G(1,i_2)]) + \\ &\quad + \ldots + 2 + f([G(1, i_{p-1}):G(1, i_p)]) = \\ &= 2p - 1 + f([F:G(1, i_p)]) = \\ &= p + f(p) + f([F:G(1, k)]) = \\ &= p + f([G:F]) + f([F:G(1, k)]) = \\ &= p + f([G:G(1, k)]) = p + f(n), \end{aligned}$$

and the proof is finished.

DEFINITION 6. Let X be a coset of a group G, let S be a DCS of X and let m be the common modulus of S. Then

$$Ab_{MZ}(S) = \text{card}(S) - (1 + f(m))$$

will be called the Mycielski-Znám abundance of S.

Notice that $Ab_{MZ}(S)$ is only defined for DCS of cosets; the index m is considered in $X^{-1}X$.

LEMMA 7. Let X be a coset of a G, let S, T be DCS of X and let T arise from S by splitting. Then

(7.1) $$Ab_{MZ}(T) \geq Ab_{MZ}(S) + Ab_{MZ}(T - S).$$

Further, if S is an invariant DCS then

(7.2) $$Ab_{MZ}(S) \geq 0.$$

PROOF. Without loss of generality we may assume $X = G$. Then (4.2) immediately implies (7.2). To prove (7.1), denote m, n, q the common indices and k, t, u the cardinalities of S, T, $T - X$, respectively. Let $A \in S - t$. Every index of T is either an index of S or the product of $[G:A]$ and an index of $T - S$. (The indices of $T - S$ are considered in $A^{-1}A$.) Hence $n \mid mq$, what together with $t = k + u - 1$ gives

$$\begin{aligned} \mathrm{Ab}_{MZ}(T) &= t - (1 + f(n)) \geq (k + u - 1) - (1 + f(mq)) = \\ &= k - (1 + f(m)) + u - (1 + f(q)) = \\ &= \mathrm{Ab}_{MZ}(S) + \mathrm{Ab}_{MZ}(T - S). \end{aligned}$$

THEOREM 8. Let S be a non-natural DCS of a cyclic group G, let $k = \mathrm{card}(S)$, let n be the common index of S and let p_3 be the third smallest prime divisor of n. Then

$$k \geq p_3 + f(n). \tag{8.1}$$

PROOF. Let $S_0, S_1, \ldots, S_u$ be a maximal splitting sequence for S. By Lemma 7 we have

$$\mathrm{Ab}_{MZ}(S) \geq \mathrm{AB}_{MZ}(S_1 - S_0) + \ldots + \mathrm{Ab}_{MZ}(S_u - S_{u-1}),$$

where all members on the right-hand side are nonnegative. Further, since S is non-natural there is an $i \in \{1, \ldots, n\}$ such that the DCS $S_i - S_{i-1}$ is non-natural; choose such an i. By Theorem 5 we have $\mathrm{Ab}_{MZ}(S_i \dot{-} S_{i-1}) \geq q - 1$, where

q is the greatest prime divisor of the common index m of DCS $S_i - S_{i-1}$. Since $m|n$ and m has at least three prime divisors we have

$$Ab_{MZ}(S) \geq Ab_{MZ}(S_i - S_{i-1}) \geq q - 1 \geq p_3 - 1,$$

what immediately implies (8.1).

REMARK: 1. The word "cyclic" in Theorem 8 can be neither deleted nor replaced by the assumption that p_3 exists. There is a counterexample (5.1) on the group $G = Z_2^3 \times Z_{15}$; its indices are 3, 3, 15, 15, 15, 15, 60, 60, 60, 60, and the groups G_i with the index 60 are pairwise distinct. Maybe, "cyclic" could be replaced by "abelian" in Theorem 5.

2. The condition "S is non-natural" can be replaced by "there is a non-natural maximal splitting sequence for S". For example, the natural DCS consisting of all 30 residue classes modulo 30 satisfies this condition.

REFERENCES

[1] M.A. BERGER, A. FELZENBAUM, S. FRAENKEL: New results for covering systems of residue classes, *Bull. Amer. Math. Soc.* 14 (1986), 121-125.

[2] I. KOREC: On a generalization of Mycielski's and Znám's hypotheses about coset decomposition of abelian groups, *Fund. Math.* 85 (1974), 41-48.

[3] I. KOREC: Irreducible disjoint covering systems, *Acta Arithm.* 44 (1984), 389-395.

[4] I. KOREC: Imrpovement of Mycielski's inequality for nonnatural disjoint covering systems of Z, *Discr. Math.* 64 (1987), 27-38.

[5] J. MYCIELSKI, W. SIERPINSKI: Sur une properiété des ensembles linéaires, *Fund. Math.* 58 (1966), 143-147.

[6] Š. PORUBSKÝ: Natural exactly covering systems of congruences, *Czech. Math. J.* 24 (1974), 598-606.

[7] Š. PORUBSKÝ: Results and problems on covering systems of residue classes, *Mitt. Math. Semin. Giessen* 150 (1981), 1-85.

[8] Š. ZNÁM: A survey of covering systems of congruences, *Acta Math. Univ. Comen.* 40-41 (1982), 52-79.

KOREC, I.

Mathematical Institute of Slovak Academy of Sciences,
Obrancov mieru 49, 814 73 Bratislava,
Czechoslovakia

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

LAWS OF THE ITERATED LOGARITHM FOR ADDITIVE FUNCTIONS

MANSTAVIČIUS E.

1. INTRODUCTION

The most of investigations in probabilistic number theory is devoted to the convergence of distributions generated by arithmetic functions. The purpose of the present paper is to call one's attention to analogues of probability theorems formulated in terms of event occurence with probability of one (almost sure occurence). Among the results we can reckon only proposition 6 from P. Erdős' paper [1] and theorem 7.2 J. Kubilius' monograph [2]. More systematic investigations can be found in our papers [3 - 6] and in short communications [7-11].

Our interest is attached to additive function $h:\mathbb{N}\to\mathbb{R}$ as well as to sequence

$$\{h_k(m) \overset{\text{def}}{=} \sum_{p\le k} h^{(p)}(m);\quad k\ge 2\}$$

where $h^{(p)}(m)=h(p^\alpha)$ if $p^\alpha||m$ and $h^{(p)}(m)=0$ otherwise. Here and in the following p stands for a prime number, $\alpha\in\mathbb{N}$. Put $\nu_n(\dots)=n^{-1}\,\#\{m\le n;\dots\}$. Denote $u^*=\operatorname{sgn} u$ if $|u|\ge 1$ and $u^*=u$, if $|u|<1$. Let ζ_p be independent random variables geting values h(p) and 0 with probabilities 1/p and 1-1/p respectively. The constants in the symbol << are considered to be absolute.

All the proofs given below are based on a truncation procedure and the following lemmas.

LEMMA 1. Let $\tau=\tau(n)\to\infty$, $\log\tau=o(\log n)$ when $n\to\infty$ and $P_i\subset\{p;p\le\tau\}$, i=1,...,s. Then uniformly in $B\subset\mathbb{R}^s$ and $s\ge 1$

$$\nu_n\Big(\Big(\sum_{p|m,\,p\in P_1} h(p),\dots,\sum_{p|m,\,p\in P_s} h(p)\Big)\in B\Big)=$$

$$=P\Big(\Big(\sum_{p\in P_1}\zeta_p,\dots,\sum_{p\in P_s}\zeta_p\Big)\in B\Big)+o(1)\quad\text{as } n\to\infty\ .$$

The proposition represents one of the versions of the Kubilius Fundamental lemma [2].

LEMMA 2. Let $p_1,\dots,p_M$ be any rearrangement of the primes up to n, $M=\Pi(n)$. For arbitrary constants $c_1\geq c_2\geq \dots\geq c_M>0$, $u>0$ and $0<M_1\leq M$ we have

$$\nu_n\Big(\max_{M_1\leq k\leq M} c_k\Big|\sum_{i\leq k} h^{(p_i)}(m)-\sum_{i\leq k} h(p_i)/p_i\Big|\geq u\Big) \ll$$

$$\ll u^{-2}\Big(c_{M_1}^2\sum_{i\leq M_1} h^2(p_i)/p_i+\sum_{M_1<i\leq M} c_i^2\,h^2(p_i)/p_i\Big).$$

The inequality is an easy modification of theorem 4.1 from I.Z. Ruzsa's preprint [12].

2. A NEW FORM OF THE ERDÖS-WINTNER THEOREM

As we have noted in paper [3] the celebrated Erdös-Wintner theorem [13] has another form.

THEOREM 2.1 /[3]/. The following propositions are equivalent:

(I) for every $\varepsilon>0$

$$a(\varepsilon)\stackrel{def}{=}\lim_{n_1\to\infty}\limsup_{n\to\infty}\nu_n\,(\max_{n_1\leq k\leq n}|h(m)-h_k(m)|\geq\varepsilon)=0;$$

(II) series

$$\sum_p h^*(p)/p, \qquad \sum_p h^{*2}(p)/p$$

converge.

Arguments form the proof of theorem 2.2 below can be repeated to show us that always a ϵ =0 or a(ϵ) = 1 (the zero-one law). Therefore proposition (I) can be used to determine convergence of $h_k(m)$ to h(m) "for almost all m" when $k\to\infty$. In the following we shall use a more general definition.

DEFINITION Let b_k, $a_{kn} \in \mathbb{R}$, $b_k>0$. We say that $b_k(h(m)-h_k(m)-a_{kn})$ tends to zero almost everywhere if for every $\epsilon>0$

$$\lim_{n_1\to\infty} \limsup_{n\to\infty} \nu_n \left(\max_{n_1\leq k\leq n} b_k|h(m)-h_k(m)-a_{km}|\geq\epsilon\right)=0.$$

For the sake of convenience the last statement we express as

$$b_k(h(m)-h_k(m)-a_{kn}) \Rightarrow 0 \text{ a.e.}$$

This new definition enables us to estimate the converegence rate of $h_k(m)$ to h(m) a.e.. At first, we point out a fairly simple approach.

Let $b_k \uparrow \infty$ as $k\to\infty$. According to theorem 2.1 convergence of series

$$(1) \qquad \sum_p (b_p h(p))^*/p, \quad \sum_p (b_p h(p))^{*2}/p$$

yields

$$g_k(m) \stackrel{def}{=} \sum_{k<p\leq n} b_p h^{(p)}(m) \Rightarrow 0 \quad a.e.$$

Now by the Abel summation due to monotonicity of b_k we come to inequality

$$b_k \left| \sum_{k<p\leq n} h^{(p)}(m) \right| \leq 2 \max_{k\leq \ell\leq n} |g_\ell(m)|$$

So from the convergence of series (1) we obtain

(2) $\quad b_k(h(m) - h_k(m)) \Rightarrow 0 \quad a.e.$.

When only the second of series (1) converges one must use centralising sequences. But such approach does not yield the exact order of the convergence rate. For some classes of functions $h(m)$ it can be found by use of corresponding results of probability theory.

Put for the sake of brevity $Lu = \log \max\{e,u\}$,

$$A(k) = \sum_{p\leq k} h(p)/p, \quad B^2(k) = \sum_{p\leq k} h^2(p)/p, \quad U_k^2 = \sum_{p>k} h^2(p)/p,$$

$$A_{kn} = A(n) - A(k), \quad v_k^2 = 2LLU_k^2, \quad R_{kn}(m) = U_k^{-1} v_k^{-1} (h(m) - h_k(m) - A_{kn}).$$

THEOREM 2.2 Let $u_n > 0$ for every $n \in \mathbb{N}$. Suppose that for $n \to \infty$ and some sequence $\tau = \tau(n)$, $\log \tau = o(\log n)$, we have

$$\rho_n \stackrel{def}{=} \sum_{\tau<p\leq n} h^2(p)/pu^2_p = o(v_\tau^2)$$

and $u_n \to 0$. If $h(p)=o(U_p v_p^{-1})$ as $p\to\infty$ then for every $\epsilon>0$

$$(3) \qquad \lim_{n_1\to\infty} \limsup_{n\to\infty} \nu_n\Big(\max_{n_1\leq k\leq n} |R_{kn}(m)| \geq 1+\epsilon\Big) = 0$$

and for every $a\in[-1,1]$

$$(4) \qquad \lim_{n_1\to\infty} \liminf_{n\to\infty} \nu_n\Big(\min_{n_1\leq k\leq n} |R_{kn}(m)-a| \leq \epsilon\Big) = 1.$$

Consequently, under the conditions of theorem 2.2 we have the exact order of the convergence rate as well as the cluster set of sequence $\{R_{kn}(m)\}$. We can say that the last one coinsides with interval $[-1,1]$ a.e..

PROOF OF THEOREM 2.2. As in convergence (2) values $h(p^\alpha)$ for $\alpha\geq 2$ have no influence on the final result. In fact, for every $\delta>0$

$$\nu_n\Big(\max_{n_1\leq k\leq n} \sum_{\substack{k<p\leq n,\alpha\geq 2\\ p^\alpha \| m}} (|h(p^\alpha)| + |h(p)|) \geq \delta\Big) \leq$$

$$\leq \nu_n\,(m; \exists p^\alpha \| m,\ \alpha\geq 2,\ n_1\leq p\leq n) << \sum_{n_1\leq p\leq n} p^{-2} = o(1)$$

when $n\to\infty$ and $n_1\to\infty$. Therefore in the following we consider only the case when $h(p^\alpha)=h(p)$ for every $\alpha\geq 1$ and p.

Let ν_1 and ν_2 be frequences in equalities (3) and (4) respectively. From lemma 2 with reverse rearragement of primes $n_1<p\leq n$ we have

$$\Delta_n(\delta) \stackrel{def}{=} \nu_n(\max_{\tau<k\leq n} |R_{kn}(m)| \geq \delta) << \rho_n/\delta^2 v_\tau^2 = o(1)$$

as $n\to\infty$. Whence

$$\nu_1 \leq \nu_n \Big(\max_{n_1\leq k\leq \tau} |R_{kn}(m)| \geq 1+\epsilon \Big) + \Delta_n(1+\epsilon) \leq$$

$$\leq \nu_n \Big(\max_{n_1\leq k\leq \tau} |h_\tau(m)-h_k(m)-A_{k\tau}|U_k^{-1}v_k^{-1} \geq 1+\epsilon/2 \Big) + (\Delta_n(\epsilon/2)+o(1)) \stackrel{def}{=}$$

(5)

$$\stackrel{def}{=} v_1' + o(1), \quad n\to\infty \ .$$

Seting $S_k = \sum_{p\geq k} \overline{\zeta}_p$ from lemma 1 we obtain

$$v_1' = P\Big(\max_{n_1\leq k\leq \tau} |S_k-S_\tau| U_k^{-1}v_k^{-1} \geq 1+\epsilon/2 \Big) + o(1) \leq$$

$$\leq P(\sup_{k\geq n_1} |S_k| \ U_k^{-1} \ v_k^{-1} \geq 1+\epsilon/4) + (P(|S_\tau| \geq \epsilon U_\tau v_\tau/4) + o(1)) \stackrel{def}{=}$$

$$\stackrel{def}{=} P_{n_1} + o(1), \quad n\to\infty \ .$$

Now by use of theorem 2 [14] we conclude that $P_{n_1}=o(1)$ when $n_1\to\infty$. This, via inequality (5), proves the first part of our theorem.

Similarly, according to lemma 1 and the theorem used

$$\nu_2\geq\nu_n\Big(\min_{n_1\leq k\leq\tau}|R_{kn}(m)-a|\leq\epsilon\Big)\geq\nu_n\Big(\min_{n_1\leq k\leq\tau}\Big|\frac{h_\tau(m)-h_k(m)-A_{k\tau}}{U_k v_k}-a\Big|\leq\frac{\epsilon}{2}\Big)+\nu_n\Big(\frac{\epsilon}{2}\Big)=$$

$$=P\Big(\min_{n_1\leq k\leq\tau}|(S_k-S_\tau)\,U_k^{-1}v_k^{-1}-a|\leq\epsilon/2\Big)+o(1)\geq$$

$$\geq P\Big(\inf_{k\geq n_1}|S_k\,U_k^{-1}v_k^{-1}-a|\leq\epsilon/4\Big)+o(1)$$

when $n\to\infty$ for every fixed $n_1\geq 2$. Theorem 2.2 is proved.

Equality (4) can be strengthened to

$$\lim_{n\to\infty}\nu_n\Big(\min_{n_1\leq k\leq n}|R_{kn}(m)-a|\leq\epsilon\Big)=1$$

for every $n_1\geq 2$ as we have seen for strongly additive functions. Is it possible to prove proposition (3) with $\epsilon=0$?

3. AN ANALOGUE OF THE FELLER THEOREM

Now we shall concider the exact growth order of the sequence $\{h_k(m)-A(k);\ k\geq 2\}$ a.e.. At first for the

comparison we quote an analogue of the Kolmogorov law of the iterated logarithm in the so-called Strassen's formulation.

THEOREM 3.1 /[4]/. Let $\beta_n \stackrel{def}{=} B(n)\sqrt{2LLB(n)} \to \infty$ and $\max_{p\leq n} |h(p)| = 0(B(n)/\sqrt{LLB(n)})$ as $n\to\infty$. Then for every $\epsilon>0$

$$\lim_{n_1\to\infty} \limsup_{n\to\infty} \nu_n \Big(\max_{n_1\leq k\leq n} \beta_k^{-1} \, | h_k(m) - A(k) | \geq 1+\epsilon \Big) = 0$$

and for every $a\in[-1,1]$

$$\lim_{n_1\to\infty} \liminf_{n\to\infty} \nu_n \Big(\min_{n_1\leq k\leq n} | \beta_k^{-1} (h_k(m) - A(k)) - a | \leq \epsilon \Big) = 1.$$

So in this case we can say that infinitely often (i.o.) for almost all (a.e.) m inequalities

$$(1-\epsilon)\beta_k \leq h_k(m) - A(k) \leq (1+\epsilon)\beta_k$$

are satisfied. Term $\epsilon\beta_k$ can be improved by use of W. Feller's paper [15]. Not trying to change its style we use normalizations

$$b_k \stackrel{def}{=} d_k \Big(\sum_{p\leq k} E\bar{\zeta}_p^2 \Big)^{1/2} = d_k \Big(\sum_{p\leq k} \frac{h^2(p)}{p}\Big(1-\frac{1}{p}\Big)\Big)^{1/2} \stackrel{def}{=} d_k D(k)$$

in the place of β_k. Here d_k stands for a monotonically

increasing to infinity sequence which would be determined. Moreover, avoiding too cumbersome conditions in this paragraph we confine ourselves to strongly additive functions satisfying

$$|h(p)| \le \lambda_p D(p) \uparrow \infty \tag{6}$$

with $\lambda_p \downarrow 0$ when $p \to \infty$.

Let us define some quantities frequently used in the large deviation theorems. Define, in a formal way, coefficients $\Gamma_{p\ell}$ by

$$\log \Big[\prod_{q \le p} \Big(1 + \frac{\exp\{th(q)\} - 1}{q}\Big) \exp\{-th(q)/q\} \Big] = \sum_{\ell=2}^{\infty} \Gamma_{p\ell} t^{\ell}/\ell!.$$

Here q denotes a prime number, $t \in \mathbb{R}$. For $|x|\lambda_p < 1/12$ under condition (6) equation

$$\sum_{\ell=2}^{r} \Gamma_{p\ell} t^{\ell-1}/(\ell-1)! = xD(p)$$

has a unique solution, say $t = t(x)$. Let $Q_p(x)$ be the function defined by

$$x^2(1+Q_p(x)) = 2 \sum_{\ell=2}^{\infty} \Gamma_{p\ell} \frac{\ell-1}{\ell!} t^{\ell}.$$

Function $Q_p(x)$ is analytic for $|x|\lambda_p < 1/12$ and for the coefficients of expansion

$$Q_p(x) = \sum_{\ell=1}^{\infty} a_{p\ell} x^{\ell} = \frac{1}{3D^3(p)} \sum_{q \le p} \frac{h^3(q)}{q} \left(1 - \frac{3}{q} + \frac{2}{q^2}\right) x + \ldots$$

estimates

$$|a_{p\ell}| \le (12\lambda_p)^{\ell}/7, \quad \ell = 1,2,\ldots$$

are known /s.f. [15]/.

THEOREM 3.2. Suppose condition (6) is satisfied, $d_p \ge 2$, $d_p \uparrow \infty$ when $p \to \infty$ and

(7) $$\lambda_p \le 1/200\, d_p.$$

The following propositions are true:

(I) if series

(8) $$\sum_p \frac{h^2(p) d_p}{p\, D^2(p)} \exp\left\{-\frac{d_p^2}{2}\left(1+Q_p(d_p)\right)\right\}$$

converges, then

$$\lim_{n_1 \to \infty} \limsup_{n \to \infty} \nu_{n_1,n} \overset{\text{def}}{=} \lim_{n_1 \to \infty} \limsup_{n \to \infty} \nu_n$$

$$\left(\max_{n_1 \le k \le n} b_k^{-1} |h_k(m) - A(k)| \ge 1 \right) = 0 \ ;$$

(II) if $\lim_{n_1\to\infty} \liminf_{n\to\infty} \nu_{n_1,n} = 0$,

then series (8) converges;

(III) if series (8) diverges, then for every $n_1 \geq 2$

$$\lim_{n\to\infty} \nu_n \left(\max_{n_1\leq k\leq n} b_k^{-1} \left| h_k(m) - A(k) \right| \geq 1\right) = 1;$$

(IV) if $\lim_{n_1\to\infty} \limsup_{n\to\infty} \nu_{n_1,n} = 1$,

then series (8) diverges.

COROLLARY /[10]/. If in the place of condition (7) estimate

$$\lambda_p = 0(d_p^{-3})$$

is satisfied, then the propositions of the theorem are true after the change of series (8) by

$$\sum_p \frac{h^2(p)d_p}{pD^2(p)} \exp\{-\frac{d_p^2}{2}\}.$$

PROOF OF THEOREM 3.2. Choose $\tau = \max$ $\{\log n, \exp\{d_n^{-1} \log n\}\}$. Then conditions (6) and (7) yield

$$D^2(n) - D^2(\tau) \ll D^2(n)\, d_n^{-2} \log \frac{\log n}{\log \tau} \leq D^2(n) d_n^{-2} \log d_n.$$

Therefore $2D^2(\tau) \geq D^2(n)$, when n is large enough. Now from

lemma 2 we have

$$\Delta_n \stackrel{def}{=} \nu_n \left(\max_{\tau \le k \le n} b_k^{-1} |h_k(m) - A(k)| \ge 1 \right) <<$$

(9)

$$<< d_\tau^{-2} + \sum_{\tau < p \le n} \frac{h^2(p)}{pb_p^2} << d_\tau^{-2} = o(1), \quad n \to \infty .$$

Whence seting $\eta_k = \sum_{p \le k} \overline{\zeta}_p$ and using lemma 1 for $n \to \infty$ we obtain

$$\nu_{n_1,n} \ge \nu_n \left(\max_{n_1 \le k \le \tau} b_k^{-1} |h_k(m) - A(k)| \ge 1 \right) + \Delta_n =$$

(10)

$$= P\left(\max_{n_1 \le k \le \tau} | b_k^{-1} | \eta_k | \ge 1 \right) + o(1) = W_{n_1} + o(1)$$

and

(11)

$$\nu_{n_1,n} \ge \nu_n \left(\max_{n_1 \le k \le \tau} b_k^{-1} | h_k(m) - A(k)| \ge 1 \right) = W_{n_1} + o(1)$$

where $W_{n_1} = P\left(\sup_{k \ge n_1} b_k^{-1} | \eta_k | \ge 1\right).$

If series (8) converges then according to the Feller theorem $W_{n_1} = 0(1)$ as $n_1 \to \infty$. This via estimate (10) proves the first proposition of our theorem. Similarly, the second one follows from estimate (11).

When series (8) diverges then by the Feller theorem $P(b_k^{-1}|\eta_k| \geq 1 \text{ i.o.})=1$. Consequently, $W_{n_1}=1$ for every $n_1 \geq 2$ and estimate (11) yields statement (III) of our theorem.

The condition of the last proposition of theorem 3.2 and estimate (10) yield asymptotic $W_{n_1}=1+o(1)$ as $n_1 \to \infty$. This due to the quoted probabilistic theorem proves the divergence of series (8). Theorem 3.2 is proved.

For example, we note that for every $s \geq 4$ and $\delta>0$

$$(2L_2k(L_4k+\frac{3}{2}L_5k+L_6k+\ldots+(1-\delta)L_sk))^{1/2} \leq \sum_{p \leq k, p|m} 1-L_2k \leq$$

$$\leq (2L_2k(L_4k+\frac{3}{2}L_5k+L_6k+\ldots+(1+\delta)L_sk))^{1/2} \text{ i.o. a.e. .}$$

Here $L_{k+1}U=L(L_kU)$ for $k \geq 1$.

It is easy to see that theorems 3.1 and 3.2 contain the zero-one law for the possible iterated limits of the frequences considered. The following problem arises: to prove an analogue of the zero-one law without any preliminary condition on additive functions and normalizations.

4. A THEOEM OF THE CHUNG TYPE

Let us consider sequence

$$\{f_k(m) \stackrel{\text{def}}{=} \max_{\ell \le k} |h_\ell(m) - A(\ell)|;\ k \ge 2\} .$$

Using the monotonicity of β_k from theorem 2.1 one can obtain information expressed by

$$1 - \varepsilon \le \liminf_{k \to \infty} \sup \beta_k^{-1} f_k(m) \le 1+\varepsilon \quad \text{a.e.} .$$

However, fairly frequently $f_k(m)$ takes much smaller values than β_k. The following theorem represents an analogue of the Chung law of the iterated logarithm.

Put for the sake of brevity $\gamma_k = \sqrt{B(k)/(8LLB(k))}$.

THEOREM 4.1. Let $h(p)=o(\gamma_p)$ and $B(p)\to\infty$ as $p \to \infty$. Then for every $\varepsilon>0$

$$(12) \quad \lim_{n_1 \to \infty} \limsup_{n \to \infty} \nu_n\Big(\min_{n_1 \le k \le n} f_k(m)/\gamma_k \le 1-\varepsilon\Big) = 0$$

but

$$(13) \quad \lim_{n_1 \to \infty} \liminf_{n \to \infty} \nu_n\Big(\min_{n_1 \le k \le n} f_k(m)/\gamma_k \le 1 + \varepsilon\Big) = 1.$$

PROOF. For every $K>0$ and $\delta>0$ we have

$$\delta_n \stackrel{\text{def}}{=} \nu_n\Big(\max_{n_1 \le k \le n} \gamma_k^{-1} \sum_{\substack{p^\alpha \| m \\ p \le k, \alpha \ge 2}} (|h(p^\alpha)| + |h(p)|) \ge \delta\Big) =$$

$$\leq \nu_n \Big(\sum_{p^\alpha \| m,\ p^\alpha \leq K} (|h(p^\alpha)| + |h(p)|) \geq \delta \gamma_{n_1} \Big) +$$

$$+ \nu_n (m; \exists p^\alpha \| m,\ p^\alpha > K, \alpha \geq 2) << o(1) + \sum_{p > \sqrt{K}} p^{-2}$$

when $n \to \infty$ and $n_1 \to \infty$. Consequently, using the standard way we can confine ourselves to strongly additive functions. Now we repeat the truncation procedure. Let $\tau = \max\{\log n, \exp\{\log n / LLB(n)\}\}$, then $B(\tau) = B(n)(1+0(1))$ as $n \to \infty$. By $\mu^-_{n_1,n}$ and $\mu^+_{n_1,n}$ we denote the frequences in equalities (12) and (13) respectively. Let η_k be random variables defined in paragraph 3. By use of lemma 1 we have

$$\mu^-_{n_1,n} \leq \nu_n \Big(\min_{n_1 \leq k \leq \tau} f_k(m)/\gamma_k \leq 1 - \varepsilon \Big) + \nu_n \Big(\min_{\tau \leq k \leq n} f_k(m)/\gamma_k \leq 1 - \varepsilon \Big) \leq$$

$$\leq P\Big(\min_{n_1 \leq k \leq \tau} \Big(\gamma_k^{-1} \max_{\ell \leq k} |\eta_\ell| \Big) \leq 1 - \varepsilon \Big) + o(1) +$$

(14)

$$+ \nu_n \Big(\max_{\ell \leq \tau} |h_\ell(m) - A(\ell)| \leq (1-\varepsilon)\gamma_n \Big) = P\Big(\inf_{k \geq n_1} \Big(\gamma_k^{-1} \max_{\ell \leq k} |\eta_\ell| \Big) \leq 1 - \varepsilon \Big) +$$

$$+ P\Big(B^{-1}(\tau) \max_{\ell \leq \tau} |\eta_\ell| \leq (1-\varepsilon)\gamma_n B^{-1}(\tau) \Big) + o(1), \quad n \to \infty.$$

According to A.I. Martikainen's theorem [16] the first probability in the right side tends to zero when $n \to \infty$. The second one by the well-known functional limit theorem can be approximated with $o(1)$ error by

$$\frac{4}{\pi} \sum_{k=1}^{\infty} \frac{(-1)^k}{2k+1} \exp\left\{-\frac{\pi^2(2k+1)^2}{8(1-\varepsilon)} \frac{B^2(\tau)}{\gamma_n^2}\right\}.$$

The last quantity due to $\gamma_n / B(\tau) = o(1)$ tends to zero when $n \to \infty$. So from estimates (14) we obtain the first statement of the theorem.

For $\mu^+_{n_1,n}$ we have

$$\mu^+_{n_1,n} \geq \nu_n\Big(\min_{n_1 \leq k \leq \tau} f_k(m)/\gamma_k \leq 1+\varepsilon \Big) =$$

$$= P\Big(\inf_{k \geq n_1} \big(\gamma_k^{-1} \max_{\ell \leq k} |\eta_\ell|\big) \leq 1 + \varepsilon \Big) + o(1)$$

as $n \to \infty$. But even

$$P\Big(\liminf_{n_1 \to \infty} \big(\gamma_k^{-1} \max_{\ell \leq k} |\eta_\ell|\big) \leq 1 + \varepsilon \Big) = 1$$

/s.f. [16]/, therefore for strongly additive function $h(m)$

$$\lim_{n \to \infty} \mu^+_{n_1,n} = 1 \tag{15}$$

when $n_1 \geq 2$ is fixed. Remembering the estimate of δ_n we obtain equality (13). Theorem 4.1 is proved.

The proposition (13) can be strengthend to (15) without the extra hypothesis of strong additivity. This can be done using a more general version of the Fundamental lemma [2]. Some other form can be given to the conditions of theorem 4.1 /s.f. [16]/.

In [5] we have laws of the iterated logarithm for additive functions not necessarilly belonging to the H class of Kubilius [2]. Nevertheless, investigation of sequences

$$\{ \sum_{p|m,\ p\leq k} \log^c p;\ k \geq 2 \}$$

with $c>0$ remains problematic.

REFERENCES

[1] ERDŐS P. On the distribution function of additive functions, *Ann. of Math.*, 47 (1946), 1-20.

[2] KUBILIUS J. *Probabilistic methods in the theory of numbers*, Gos. Izdat. Polit. Naučn. Lit. Litovsk. SSR, Vilnius, 1962; English transl., Transl. Math. Monographs, vol. 11, Amer. Math. Soc., Providence, R.I., 1964.

[3] MANSTAVIČIUS E. Strong convergence of additive arithmetic functions, *Litovsk. Mat. Sbornik* (Russian), 25, 2 (1985), 127-137.

[4] MANSTAVIČIUS E. Law of the iterated logarithm in the Strassen formulation and additive functions, *Litovsk. Mat. Sbornik* (Russian), 26, 1 (1986), 81-90.

[5] MANSTAVIČIUS E. Two laws of the iterated logarithm for additive functions, *Litovsk. Mat. Sbornik* (Russian), 26, 2 (1986), 283-291.

[6] MANSTAVIČIUS E. Sums of additive arithmetic functions with shifted arguments (in Russian), *Analytic Number Theory*, Petrozavodks O.V. Kuusinen State Univ., 1986, 51-60.

[7] MANSTAVIČIUS E. Law of the iterated logarithm for additive functions (in Russian), The XXV-th conference of the *Lith. Math. Soc. Abstracts of Comm.*, Institut of Math. and Cybern. of the Acad. Sci. Lith. SSR, 1984, 175-176.

[8] MANSTAVIČIUS E. The law of iterated logaritm in probabilistic number theory, *Fourth International Vilnius Conf. on Probab. Th. and Math. Statistics*, Abstracts of Comm., Inst. of Math. and Cybern. of the Acad. Sci. Lith. SSR, 1985, t. IV, 193-194.

[9] MANSTAVIČIUS E., MUSNIKAITĖ R. Additive functions on ordered semigroups with regular norms (in Russian),

The XXVI-th Conf. of the Lith. Math. Soc., Abstracts of Comm., Inst. of Math. and Cybern. of the Acad. Sci. Lith. SSR, 1985, 179-180.

[10] MANSTAVIČIUS E. Maximums of sequences of additive functions (in Russian), *Abstracts of Comm. of Allunion Conf.* "Number Theory and its Applications", Tbilisi, 1985, 150-153.

[11] MANSTAVIČIUS E. The zero-one law in probabilistic number theory (in Russian), *The XXVII-th Conf. of the Lith. Math. Soc., Abstracts of Comm.*, Vilnius V. Kapsukas State Univ., 1986, t.1, 17-18.

[12] RUZSA I.Z. Effective results in probabilistic number theory, *Preprint of the Math. Inst. of the Acad. Sci. Hung.*, 12 (1982), 24 p.

[13] ERDŐS P., WINTNER A. Additive arithmetical functions and statistical independence, *Amer. J. Math.*, 61, 3 (1939), 713-721.

[14] KLESOV O.I. On the convergence rate of series of random variables, *Ukrain.Math.J.* (Russian), 35, 3 (1983), 309-314.

[15] FELLER W. The general form of the so-called law of the iterated logarithm, *Trans. Amer. Math. Soc.*, 54 (1943), 373-402.

[16] MARTIKAINEN A.I. On the Chung law for nonidentically distributed independent summands, *Teoria Verojatn. i ee Prim.* (Russian), 26, 3 (1986), 566-568.

MANSTAVIČIUS, E.
Dept. of Probability Theory
and Number Theory
Faculty of Maths.
Partizanu 24
232006. Vilnius. USSR

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE SUM OF ABSOLUTE VALUES OF COEFFICIENTS OF SOME ARTIN L-FUNCTIONS ASSOCIATED WITH RATIONAL CHARACTERS

MARKO F.

Moroz in [8] proved the mean value theorem with remainder term for the sum $\sum_{n\leq x} a_n$ of coefficients of scalar product of the Artin-Weil L-functions. The task of determination of the mean value of the sum $\sum_{n\leq x}|a_n|$ of absolute values of coefficients of Artin L-function arises in connection with the lower bound for the number of its zeroes on the critical line (see [11] and [3]). We determine this mean value for some Artin L-functions associated with rational character.

Let Q be the field of rational numbers, K be an algebraic number field and L be the Galois closure of K with Galois group G.

In what follows we shall always suppose that χ is

an character of a linear representation of the group G realizable over Q and $\Phi(s)$ is the Artin L-function associated with this rational group character.

1. DECOMPOSITION OF ARTIN L-FUNCTION

Let

$$A_i(s) = \prod_{p \in M_i} (1 - p^{-s})^{-1},$$

where M_i is a set of primes unramified in L which have the same decomposition type (i.e. they have the same associated Artin symbol in L and hence the same number of prime divisors, each with the same residue class of the degree f and ramification index e) in the subfields K_j of the field L corresponding to a system of representatives $\{C_1, \ldots, C_g\}$ for the conjugacy classes of cyclic subgroups of G. The number of such sets M_i equals the number of conjugacy classes of cyclic subgroups of G.

The same arguments as for Riemann zeta function yield that every $A_i(s)$ converges in the half-plane $\sigma > 1$.

According to Theorem 30 and Exercise 13.8 of [9] (see also Remark 2 on p.104) every Artin L-function relative to a character realizable over Q (as a special case the zeta function of the subfield F of L) can be uniquely expressed as a product of fractional powers of zeta functions of the subfields $K_1, \ldots, K_g$ (corresponding

to subgroups $C_1, \ldots, C_g$, respectively).

It can be shown (see [9], Remark 1 on p.104) that the analogous theorem does not hold for integer exponents even if K_j runs through all subfields of L.

We may write

$$\Phi(s) = \prod_j \zeta_{K_j}(s)^{b_j} .$$

Every $\zeta_{K_j}(s)$ can be expressed in the form

$$\zeta_{K_j}(s) = \prod_i A_i(s)^{h_{ij}} \phi_j(s),$$

where $\phi_j(s)$ is analytic for $\sigma>1/2$. This may be done in the same way as in [1].

Let $H = ||h_{ij}||_{gxg}$. Suppose that the rank of the matrix H is $t \leq g$ and $i_1, \ldots, i_t$ are indices of linearly independent rows of H. We can find indices $j_1, \ldots, j_t$ such that the matrix $H_0 = ||h_{i_k j_l}||_{txt}$ is regular.

REMARK 1: Suppose that the field L has a squarefree order over Q. Let G_Z denote the decomposition group of a unramified prime p in L. If F_Z is the fixed field of G_Z, then p splits in a field $F \subset L$ on $[F \cap F_Z:Q]$ prime divisors of degree $[F:F \cap F_Z]$ because of a squarefree order of L. If we order the set of cyclic subgroups of G in such a way that a group with a smaller order preceeds a group with a greater one and the fields K_Z in the same way as the groups G_Z, we see immediately that the functions

$A_i(s)$ are linearly independent, because H forms a square triangle matrix.

From the system of linear equations corresponding to the matrix H_0 we may determine $A_{i_k}(s)$ as the product of the fractional powers of the functions $\zeta_{Kj}(s)$ multiplied by the function, which is analytic and nonzero for $\sigma>1/2$.

Since every row of H is a linear combination of the rows $i_1, \ldots, i_t$, we may express each $A_i(s)$ in the form

$$A_i(s) = \prod_j \zeta_{Kj}(s)^{d_{ij}} \phi_i(s)$$

with rational d_{ij} and functions $\phi_i(s)$ analytical and nonzero for $\sigma>1/2$.

From this decomposition we obtain the "order" d_i of the function $A_i(s)$ at s=1, i.e. for $d_i = \sum_j d_{ij}$ we have that $(s-1)^{d_i} A_i(s)$ is analytical for $\sigma>1/2$.

Therefore we may write

$$\Phi(s) = \prod_j \zeta_{Kj}(s)^{b_j} = \prod_j \prod_i A_i(s)^{h_{ij}b_j} \phi_j(s) =$$

$$= \prod_i A_i(s)^{\sum_j b_j h_{ij}} \phi(s),$$

where $\phi(s)$ is analytic for $\sigma>1/2$.

2. THEOREM

The main result of this paper is the following

THEOREM: Let $\Phi(s)$ be an Artin L-function associated with a rational character χ and

$$\sum_{m=1}^{\infty} \alpha(m) m^{-s}$$

be the Dirichlet serie for $\Phi(s)$ $(\sigma>1)$. If the exponents $\sum_j b_j h_{ij}$ of $A_i(s)$ in the above expression for $\Phi(s)$ are positive rational or negative integer numbers (the special case is when $\Phi(s)$ is a product of positive rational or integer powers of Dedekind ζ-functions of the subfields of the field L), the for $d = \sum_i d_i \left| \sum_j b_j h_{ij} \right|$ and some positive B_1 we have

$$\sum_{1 \le m \le x} |\alpha(m)| \sim B_1 x (\ln x)^{d-1}.$$

REMARK 2. The asymptotic values of certain coefficients sums for $\Phi(s) = \zeta_K(s)/\zeta(s)$ where K is a nonabelian cubic field were determined in [2].

Function determined by Dirichlet serie $\sum_m |\alpha(m)| m^{-s}$ $(\sigma > 1)$ will be denoted by $\psi(s)$.

3. PROPERTIES OF THE FUNCTION $\psi(s)$

LEMMA 1: Let $B(s) = \sum_{n=1}^{\infty} b_n n^{-s} = \prod_{p \in M} (1-p^{-s})^{-1}$ and

$A(s) = \sum_{n=1} a_n n^{-s}$ be Dirichlet series. Denote

$$A_a(s) = \sum_{n=1}^{\infty} |a_n| n^{-s}.$$

If α is positive rational, then

$$(B^{\alpha})_a(s) = B^{\alpha}(s).$$

If α is negative integer, then

$$(B^{\alpha})_a(s) = B^{-\alpha}(x) B^{\alpha}(2s).$$

PROOF:

$$B^{\alpha}(s) = (\prod_{p \in M} (1-p^{-s})^{-1})^{\alpha} = \prod_{p \in M} (1-p^{-s})^{-\alpha}$$

converges in the half-plane $\sigma > 1$.

Since Dirichlet serie is uniquely determined by its coefficients, it is sufficient to prove the above statement for the expressions $(1-p^{-s})^{-\alpha}$ considered as a formal infinite series of unknown $x = p^{-s}$.
But $(1-p^{-s})^{-1} = 1 + p^{-s} + \ldots + p^{-ks} + \ldots$ and

$$(1-p^{-s})^{-\alpha} = 1 + \binom{-\alpha}{1} (-p)^{-s} + \ldots + \binom{-\alpha}{k} (-p^{-s})^k + \ldots$$

If α is positive, then every term $\binom{-\alpha}{k} (-1)^k$ is positive and first part of Lemma 1 is clear.

The second part is clearly true if $\alpha = -1$. Raising to the power, one sees that the second part is also true.

If α is negative and noninteger, then the situation is more complicated and we do not investigate it.

Using results of [7] one can modify the results for Riemann zeta function (see [5] and [10]) to obtain that for some $d_i \in Q$ and positive c_1, c_2, c_3 the functions $(s-1)^{d_i} A_i(s)$ can be extended analytically to the region R defined by

$$\sigma \geq 1 - c_1(\ln\ln|t|/\ln|t|)^{2/3}, \quad \sigma \geq c_2,$$

are nonzero for s=1 and both $A_i(s)$ and $A_i^{-1}(s)$ are $O(\ell n^{c_3}|t|)$ in this region.

Using Lemma 1 and the expression for $\Phi(s)$ as a product of fractional powers of $A_i(s)$ and $\phi(s)$, we obtain that the function $(s-1)^d \psi(s)$ can be extended analytically to the region R, is nonzero at s=1 and $\psi(x) = O(\ln^{c_4}|t|)$ in this region.

This is the step where the "decomposition" of $\Phi(s)$ into a product of fractional powers of $A_i(s)$ is needed.

We may therefore write

$$\psi(s)/s = (s-1)^{-d}(A_0 + A_1(s-1) + A_2(s-1)^2 + \ldots)$$

4. COMPLEX INTEGRATION

To complete the proof of the theorem we will use the method of complex integration (see [6], p.271-273).

At first stage we have

$$(1/2\pi i)\int_{2-x^3 i}^{2+x^3 i} \psi(s)x^s/s\, ds = \sum_{1\leq m\leq x} |\alpha(m)| + O(1)$$

At second stage we proceed similarly as [4], p.653-658. We shortly reproduce the necessary results. For x sufficiently large we use Cauchy's theorem to change the path of integration in the integral on the left side as follows:

1. From $A = 2+x^3 i$ to $B = U(x) + x^3 i$
2. From B to $C = U(x)$
3. From C to $D = 1 - \delta$ on the upper half-plane
4. From D to D on the circle with centre $s = 1$ and radius δ in clockwise order
5. From D to C on the lower half-plane
6. From C to -B
7. From -B to -A

where $U(x) = 1 - c_1(\ln\ln x^3/\ln x^3)^{2/3}$ and δ is chosen smaller than $1 - U(x)$.

The contribution to the integral from the path 1. and 7. is $\sigma(1)$.

The contribution from path 2. and 6. is $O(x^{U(x)})$.

The contribution from the paths 3.,4. and 5. is

$$(1/2\pi i)A_0\int_0^0 x^s(s-1)^{-d}\, ds + O\int_0^1 x^s(1-s)^{1-d}\, ds + O(x^{U(x)})$$

if d is not an integer, resp. $\operatorname{res}_{s=1} \psi(s)x^s/s$ if d is an integer.

In the above relation the first integral is taken on the following path:

1. From 0 to $1 - \delta$ on the upper half-plane
2. From $1 - \delta$ to $1 - \delta$ on the circle with centre s=1 and radius δ in clockwise order
3. From $1 - \delta$ to 0 on the lower half-plane

For $0 < \eta < 1$ we have

$$\int_0^0 x^s(s-1)^{-\eta}\, ds = (e^{-\pi i\eta} - e^{\pi i\eta}) \int_0^1 x^s(1-s)^{-\eta}\, ds$$

and

$$\int_0^1 x^s(1-s)^{-\eta}\, ds = x(\ln x)^{\eta-1} \int_0^{\ln x} e^{-v}v^{-\eta}\, dv$$

$$\sim (x(\ln x)^{\eta-1})\, \Gamma(1-\eta) \qquad \text{(i)}$$

and therefore

$$\int_0^1 x^s(1-s)^{-\eta}\, ds = 0\,(x(\ln x)^{\eta-1}). \qquad \text{(ii)}$$

If b is not an integer, using partial integration we obtain

$$\int_0^0 x^s(s-1)^{-b}\, ds = c_5(\ln x) \int_0^1 x^s(1-s)^{1-b}\, ds + 0(1),$$

where $c_5 \neq 0$ is a constant.

Suppose that d is not an integer.

Using these equations we may estimate the integral

$$\int_0^1 x^s(1-s)^{-d}\,ds \text{ using integral } \int_0^1 x^s(1-s)^{-d+[d]}\,ds.$$

Here $0<d-[d]<1$ and we may use (i) and (ii) to obtain

$$\int_0^1 x^s(1-s)^{-d} \sim B_1 x(\ln x)^{d-1}$$

where B_1 is a positive constant.

We are not interested in the exact value of constant B_1, however, it can be explicitly determined from the above considerations.

From the above considerations follows finally the expression for the asymptotic value of the sum

$$\sum_{1\leq m\leq x} |\alpha(m)|.$$

If d is an integer, then the same result follows from the above and the computation of the corresponding residuum $\operatorname{res}_{s=1} x^s\psi(s)/s$. If d is an integer greater than 1, we obtain a better estimate than a mean value because of lower terms of magnitude $Bx(\ln x)^i$, $i = 0, \ldots, d-2$.

REMARK 3: From the above it is easy to deduce that

$$\sum_{1\leq m\leq x} \alpha(m) \sim Bx(\ln x)^{d'-1}, \text{ where}$$

$$d' = \sum_j b_j$$

is the sum of exponents in the expression for $\Phi(s)$ as a product of fractional powers of $\zeta_{K_j}(s)$. As stated in [8] d' is an integer and therefore one can find a better estimate for the sum

$$\sum_{1 \le m \le x} \alpha(m).$$

For related questions see [8].

5. EXAMPLE

The method of determination of number d introduced at the beginning of the paper we illustrate on the following example:

Let $\Phi(s) = \zeta_K(s)/\zeta(s)$ and the group G is a transitive and primitive subgroup of the group $SL(2,l^n)$, where l is prime, i.e. the situation is the same as in [1], p.150. That is, if g is a primitive root of the Galois field $GF(l^n)$ then G consists of ml^n permutations $\pi = (z, g^{ir}z+b)$ $(i=0,\ldots,m-1)$ for suitable integer m, such that $l^n-1 = mr$.

In this case we use an other system of linearly independent Dedekind zeta functions than in the proof of Theorem 1.

It can be easy verified that if $k \backslash m$, $k \neq m$, then the set of permutation $\{(z, g^{cr}z+b), k \backslash c,$ b arbitrary$\}$ forms a

normal subgroup G_k of G, and the set of permutations $\{(z,z+b),\ b \text{ arbitrary}\}$ forms a normal subgroup G_0 of G. Moreover, we denote by G_m the trivial subgroup of G consisting only of identical permutation.

Suppose that a prime p does not ramify in L. Depending on the generating permutation π of decomposition group of p in L, we obtain the following contribution of prime p to the Dedekind zeta function of the fields K_e for e\m, e≠m; K_0 and $K_m = L$; respectively, the fixed fields of the groups G_e; G_0 and G_m; respectively. (The contribution depends only on the type of the permutation, since each field K_j is normal and two permutations of the same type are conjugate):

π	K_e	K_0	K_m
$(z,g^{kr}z+b)$	$(1-p^{-sw/k})^{ek/w}$	$(1-p^{-ms/k})^{k}$	$(1-p^{-ms/e})^{1^n e}$
$(z,z+b), b\neq 0$	$(1-p^{-s})^{e}$	$(1-p^{-s})^{m}$	$(1-p^{-ls})^{1^{n-1}m}$
(z,z)	$(1-p^{-s})^{e}$	$(1-p^{-s})^{m}$	$(1-p^{-ls})^{1^{n}m}$

where $w = [k,e]$.

For e\m, e≠m; e=0; and e=m; respectively we define $A_e(s)$ as product of terms $(1-p^{-s})^{-1}$ over all primes p for which the generating permutation (of the decomposition group corresponding to p) equals $(z,g^{er}z+b)$; $(z,z+b)$, $b\neq 0$; and (z,z) respectively.

Using [1] , Hilfsatz, we see that

$$\Phi(s) = A_m^{l^n-1}(s)A_0^{-1}(s)\phi(s)$$

and therefore

$$\Psi(s) = A_m^{l^n-1}(s)A_0(s)\psi(s),$$

where $\psi(s)$ is analytic for $\sigma>1/2$.

We may write $A_e(s)$ in the form

$$A_e(s) = \prod_{\substack{t\backslash m \\ t\neq m}} \zeta_{K_t}(s)^{d_{t,e}}\zeta_{K_0}(s)^{d_{0,e}}\zeta_{K_m}(s)^{d_{m,e}}\phi_e(s).$$

Numbers $d_{i,t}$ can be determined from the systems of linear equations with the matrix

$$H = \begin{Vmatrix} 1 & \dots\dots\dots & 0 & \dots & 0 & 0 \\ \cdot & & \cdot & & \cdot & \cdot \\ \cdot & & \cdot & & e & \cdot \\ 1 & \dots\dots\dots & e & \dots & 0 & 0 \\ 1 & \dots\dots\dots & e & \dots & m & 0 \\ 1 & \dots\dots\dots & e & \dots & m & l^n m \end{Vmatrix}$$

Using Cramer's rule we obtain that

$d_{0,t} = 0$ for $t\neq m,0$, $d_{0,0} = -1/ml^n$ and $d_{0,m} = 1/m$,

$d_{m,t} = 0$ for $t\neq 0$ and $d_{m,0} = 1/ml^n$.

This means that $d_0 = (\ell^n-1)/m\ell^n$, $d_m = 1/m\ell^n$ and $d = d_m(l^n-1) + d_0 = 2(l^n-1)/ml^n$.

Therefore we have

$$\sum_{1\leq m\leq x} |\alpha(m)| \sim B_1 x(\log x)^{(2(l^n-1)/ml^n)-1}$$

REMARK 4: We can determine the numbers d_m and d_0 from an other system of linear equations. For example, since the decomposition of primes in K depending on the generating permutation π is known, it is easy to obtain the expression for $A_e(s)$ in the above form, where $\zeta_K(s)$ is used instead of $\zeta_L(s)$.

REMARK 5: Of course in this case we have (see Remark 3)

$$\sum_{1\leq m\leq x} \alpha(m) \sim Bx/\ln x.$$

REFERENCES

[1] E. ARTIN: Über die Zetafunctionen gewisser algebraischer Zahlkörper, Math.Ann. 89(1923), 147-156.

[2] P. BARRUCAND: Quelques propriétés des coefficients des séries L associées aux corps cubiques, C.R.Acad. Sci. (Paris) Sér.A-B 273(1971), A960-A963.

[3] B.C. BERNDT: The Number of Zeroes of the Dedekind Zeta-Function on the Critical Line, J. of Number Theory 3(1971), 1-6.

[4] E. LANDAU: "Handbuch der Lehre von der Verteilung der Primzahlen", Zweiter Band, *Chelsea Publishing Company*, New York 1953.

[5] E. LANDAU: "Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale", *Teubner-Verlag*, Leipzig und Berlin 1918.

[6] S. LANG: "Algebraic number theory", *Addison-Wesley*, Reading, Mass., 1970.

[7] T. MITSUI: On the prime ideal theorem, J.Math.Soc. Japan 20(1968), 233-247.

[8] B.Z. MOROZ: "Analytic aritmetic in algebraic number fields", Lecture Notes in Mathematics 1205, *Springer-Verlag* Berlin-Heidelberg 1986.

[9] J.-P. SERRE: "Linear representations of finite groups", Graduate texts in mathematics 42, *Springer-Verlag* New York 1977.

[10] E.C. TITCHMARCH: "The theory of Riemann zeta-function", *Clarendon*, Oxford 1951.

[11] L. WEINSTEIN: The Zeros of the Artin L-Series of a Cubic Field on the Critical Line, J. of Number Theory 11 (1979), 279-284.

MARKO, F.

Mathematical Institute
Slovak Academy of Sciences
Obrancov mieru 49
814 73 Bratislava,
C z e c h o s l o v a k i a

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

SUBSTITUTIVE NORMAL SETS

CHRISTIAN MAUDUIT

Let $u = (u_n)_{n\in\mathbb{N}}$ be an infinite sequence of integers. Define $B(u)$ as the set of those real α's such that the sequence $(u_n\alpha)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1. A set B of real numbers is said to be normal if there exists a sequence u such that $B = B(u)$. G. Rauzy has given a complete characterization of normal sets (cf. [4]), namely, a set B is normal if and only if (i) $0 \notin B$, $B+1=B$; (ii) $\forall\, q \in \mathbb{Z}^*$, $qB \subset B$; (iii) there exists a sequence $(f_n)_{n\in\mathbb{N}}$ of continuous real functions such that $\lim_{n\to\infty} f_n(x) = 0$ exactly for those x's which are elements of B.

We will say that a set B of real numbers is Σ-normal (or a substitutive normal set) if there exists an increasing

sequence u generated by an irreducible substitution such that $B = B(u)$. We give the following characterization of Σ-normal sets (cf. [2]):

THEOREM: B is a Σ-normal set if and only if $\mathbb{R} \setminus B$ is an algebraic extension of finite degree of $\mathbb{Q}$.

I. SUBSTITUTION OVER A FINITE ALPHABET

Let $g \geq 2$, $A = (a_1, \ldots, a_g)$ an alphabet and Σ a substitution over A (cf. [6]).

Σ is given by the set $\Sigma(a_i) = a_{\sigma_i(1)}, \ldots, a_{\sigma_i(\ell_i(1))}$ $(i \in \{1, \ldots, g\})$, where $\ell_i(n)$ is the length of the word $\Sigma^n(a_i)$ $(n \in \mathbb{N})$ and σ_i a map from $\{1, \ldots, \ell_i(1)\}$ to $\{1, \ldots, g\}$.

We will suppose that Σ is irreducible, that is to say that for any $(i,j) \in \{1, \ldots, g\}^2$, there exists an integer n such that the word $\Sigma^n(a_i)$ contains the letter a_j.

We remark that $L(n) = M^n \, {}^T(1, \ldots, 1)$, where $L(n) = {}^T(\ell_1(n), \ldots, \ell_g(n))$ and

$$M = (M_{ij})_{(i,j) \in \{1, \ldots, g\}^2} \quad \text{with} \quad M_{ij} = \operatorname{card}(\sigma_i^{-1}(\{j\})).$$

Definition: Let $m \in A^{\mathbb{N}}$ and $t \in \{1, \ldots, g\}$. We call support of m with respect to a_t and we denote by $[m]_t$, the increasing sequence of those integers n such that a_t is

the (n+1)-th letter of the word m.

We say that a sequence u of integers is generated by a substitution Σ if there exists $m \in A^{\mathbf{N}}$ such that $\Sigma(m) = m$ and $t \in \{1,\ldots,g\}$ such that u is the support of m with respect to a_t.

II. λ FUNCTIONS ASSOCIATED TO Σ

Statistical properties of sequences generated by Σ are determined by the behaviour of the following functions.

If $\sigma_i^{-1}(\{j\})$ is non empty, let us denote by $k_1,\ldots,k_{M_{ij}}$ the increasing sequence of its elements.

For any $\nu \in \{1,\ldots,M_{ij}\}$ we put $\lambda_{ij}^{(\nu)} = \sum_{k'<k_\nu} \ell_{\sigma_i(k')}$,

$$\Lambda_{ij} = \lambda_{ij}^{(\nu)},\ \nu \in \{1,\ldots,M_{ij}\} \setminus \{0\} \text{ and } \Lambda = \bigcup_{(i,j)\in\{1,\ldots,g\}^2} \Lambda_{ij}.$$

Now we define the set E:

$$E = \{\alpha \in \mathbf{R}, \exists k \in \mathbf{Z}^*,\ \forall \lambda \in \Lambda \lim_{n\to\infty} e(k\lambda(n)\alpha) = 1\}$$

(where $e(x) = \exp(2i\pi x)$) and we show that

$$E = \{\alpha \in \mathbf{R},\ \exists k \in \mathbf{Z}^*,\ \forall i \in \{1,\ldots,g\}\ \lim_{n\to\infty} e(k\ell_i(n)\alpha) = 1\}$$

is an algebraic extension of finite degree of $\mathbf{Q}$.

Example 1. If Σ is a substitution of constant length (i.e. $\ell_i(1) = r$ for any $i \in \{1,\ldots,g\}$), that is to say if u is generated by a finite automaton (cf. [1]), we have $\Lambda = \{\lambda\}$ with $\lambda(n) = r^n$, and so $E = Q$.

Example 2. If Σ is defined by $\Sigma(a_1) = a_1a_2a_2$ and $\Sigma(a_2) = a_2a_1$, we have $\Lambda_{11} = \Lambda_{22} = \emptyset$, $\Lambda_{12} = \{\ell_1, \ell_1 + \ell_2\}$ and $\Lambda_{21} = \{\ell_2\}$ with $\ell_1(0) = \ell_2(0) = 1$, $\ell_1(1) = 3$, $\ell_2(1) = 2$ and for any $i \in \{1,2\}$ $\ell_i(n+1) = 2\ell_i(n)+\ell_i(n-1)$. We deduce from this that $E = Q(\sqrt{2})$.

III. NORMAL SET WITH RESPECT TO A SUBSTITUTIVE SEQUENCE

First, we have to show that if u is generated by Σ, then $B(u) = \mathbf{R}\backslash E$. We recall that, according to Weyl's criterium (cf. [5]), the sequence $(u_n \cdot \alpha)_{n\in\mathbf{N}}$ is uniformly distributed modulo 1 if and only if, for any $k \in \mathbf{Z}^*$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n<N} e(k\, u_n \alpha) = 0.$$

Let us consider the Weyl sums $S_i(\alpha,n) = \sum_{p\in[\Sigma^n(a_i)]_t} e(p\alpha)$

and the vector $w(\alpha,n) = (w_i(\alpha,n))_{i\in\{1,\ldots,g\}}$,

with $w_i(\alpha,n) = \dfrac{S_i(\alpha,n)}{S_i(0,n)}$.

Then $w(\alpha,n+1) = A(\alpha,n)\, w(\alpha,n)$ where $A(\alpha,n)$ is a $g \times g$-matrix. We remark that every coefficient of $A(\alpha,n)$ depending on α is a real linear combination of $e(\lambda(n)\alpha)$ with $\lambda \in \Lambda$.

So, if $\alpha \in \mathbb{R}\backslash E$ the arguments of these complex numbers are "well distributed" modulo 2π, and we show that $\lim_{n\to\infty} B(\alpha,n) = 0$ (we put $B(\alpha,n) = A(\alpha,n)\, A(\alpha,n-1)\ldots$ $\ldots A(\alpha,0)$).

We deduce from this that $w(\alpha,n) \in o(1)$ and then $\sum_{p\in[m]_t} e(p\alpha) \in o(N)$, i.e. $(u_n.\alpha)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1.

Conversely, let $\alpha \in E$.
As $(A(\alpha,n) - A(0,n))$ converges to 0 with an exponential speed, $(B(\alpha,n) - B(0,n))$ is smaller than some constant related to the spectrum of M. By iterating Σ, this constant can be made arbitrarely small.

As $w(\ ,n+1) = B(\alpha,n)\, w(\alpha,n)$

$$= {}^{T}(1,\ldots,1) + (B(\alpha,n) - B(0,n))\,{}^{T}(0,\ldots,0,1,0,\ldots,0),$$

it follows that $\underline{\lim} |w_1(\alpha,n)| > 0$ and so the sequence $(u_n\cdot\alpha)_{n\in\mathbb{N}}$ is not uniformly distributed modulo 1.

IV. CONVERSE

Let F be an algebraic extension of finite degree of Q. We know that there exists a Pisot number θ such that $F = Q(\theta)$ (cf. [3]).

On the other hand, we can show that for any Pisot number θ of degree g, there exists an integer ν and an irreducible non negative integral $g \times g$ matrix $M = (M_{ij})_{(i,j)\in\{1,\ldots,g\}^2}$ such that the spectrum contains only θ^ν and its conjugates.

Now consider the substitution Σ given by

$$\forall i \in \{1,\ldots,g\},\ \Sigma(a_i) = \underbrace{a_1\ldots a_1}_{M_{i1}\text{ times}}\ldots\ldots\underbrace{a_j\ldots a_j}_{M_{ij}\text{ times}}\ldots\ldots\underbrace{a_g\ldots a_g}_{M_{ig}\text{ times}}$$

By iterating Σ, we can suppose $M_{ij} > 0$. Then, let m be the fixed point of Σ beginning with a_1 and $u = [m]_1$ be the sequence generated by m and a_1.

Using the same method as in § III, we show that $E = Q(\theta^\nu)$.

As θ is a Pisot number, $Q(\theta^\nu) = Q(\theta)$ and

$B(u) = R\backslash E = R\backslash Q(\theta^\nu) = R\backslash Q(\theta) = R\backslash F$.

So, $R\backslash F$ is a Σ-normal set.

REFERENCES

[1] C. MAUDUIT: Automates finis et ensembles normaux, *Ann. Inst. Fourier*, t. 36, fasc. 2, pp. 1-25.

[2] C. MAUDUIT: Caractérisation des ensembles normaux substitutifs, *Invent. Math.* (to appear).

[3] C. PISOT: La répartition modulo 1 et les nombres algébriques, *Ann. Scuola Normale Sup. Pisa*, vol. 7, 1938, pp. 205-245.

[4] G. RAUZY: Caractérisation des ensembles normaux, *Bull. Soc. Math. France*, vol. 98, 1970, pp. 401-414.

[5] G. RAUZY: Propriétés statistiques de suites arithmétiques, *P.U.F.*, 1976.

[6] G. ROZENBERG and A. SALOMAA: The mathematical theory of L-systems, *Academic Press*, 1980.

Christian Mauduit
C.N.R.S. L.A. 225
Université d'Aix-Marseille II
Département Mathématique-Informatique
70, route Léon-Lachamp
13288 Marseille Cedex 9
France

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE ORDER OF THE MAASS L-FUNCTION ON THE CRITICAL LINE

TOM MEURMAN

1. INTRODUCTION

Let Ψ be a Maass cusp (wave) form (see Maass [6]) corresponding to the eigenvalue $1/4 + \kappa^2$ as defined in [7]. Equivalently Ψ can be defined as follows:

1) Ψ is a complex function defined in the upper half plane H,

2) $\Psi(z) = \Psi(-1/z)$ for $z \in H$,

3) $\Psi(z) = \sum_{n \neq 0} \rho(n)\sqrt{y}\, K_{i\kappa}(2\pi|n|y)e(nx)$ for $z = x + iy \in H$,

4) $\rho(m)\rho(n) = \sum_{\substack{d|(m,n) \\ d>0}} \rho(mnd^{-2})$, $\rho(1) \neq 0$,

5) ρ is even or odd in n.

Here K is Macdonald's function and $e(x) = \exp(2\pi ix)$. We gave this definition only for the sake of completeness. The norm $\|\Psi\|$ is an in [7]. Note that we have $\rho(1) = 1$.

The Maass L-function (defined by Maass [6]) is

$$L(s) = L_\Psi(s) = \sum_{n=1}^{\infty} \rho(n) n^{-s}.$$

This converges absolutely for $\sigma = \mathrm{Re}(s) > 1$ and can be analytically continued to an entire function. Other properties will be given in Section 6.

We shall prove

THEOREM 1. *For* $t \gg 1$, $\kappa \ll t^{1/3}$ *and* $\varepsilon > 0$ *we have*

$$L_\Psi(\tfrac{1}{2} + it) \ll_\varepsilon \|\Psi\| \sqrt{\kappa} e^{\pi\kappa/2} t^{1/3+\varepsilon},$$

where the implied constant depends at most on ε.

Previously Epstein, Hafner and Sarnak [1] have given a bound with the exponent $1/2 + \varepsilon$.

The factor depending on Ψ (and κ) is determined by C_Ψ in the inequality

$$\sum_{n \le x} |\rho(n)|^2 \ll C_\Psi x . \tag{1.1}$$

Huxley [3] has shown that

$$(1.2) \qquad C_\psi \ll \kappa e^{\pi\kappa} \|\psi\|^2 .$$

For L-functions attached to holomorphic cusp forms the analogue of Theorem 1 is already known (see Good [2]). Both of these results are analogues of the classical estimate $\zeta(1/2+it) \ll t^{1/6+\varepsilon}$ for the Riemann zeta-function.

Theorem 1 will be proved by a modification of a new method of Jutila [5], applied by himself to $\zeta^2(s)$ and to L-functions attached to holomorphic cusp forms. In our case the flexibility of the method is reflected by the fact that we dispense with the "Ramanujan-Petersson conjecture" for $\rho(n)$. The method may be summarized as follows:

1) Convert the problem to the problem of estimating a "long" Dirichlet polynomial.

2) Split up this to sums over "short" intervals, each interval being in a neighbourhood of $t/2\pi r$, where r runs through a sequence of rational numbers.

3) Transform the short sums.

4) Add up the transformed sums.

5) Estimate the resulting expression.

In fact this is an outline of the last section of this paper, the rest of it serving as a preparation for the third step above.

In addition to the notation given above, let h and k be coprime integers, $k > 0$, $\bar{h}$ be defined via $h\bar{h} \equiv 1 \pmod{k}$, $r = h/k$ and $\bar{r} = \bar{h}/k$. The Bessel functions H, J and K will be as usual (see [8]). The letters A and δ will stand for some positive constants, where usually A is large and δ is small. Write $\mathrm{Re}(s) = \sigma$ and $\mathrm{Im}(s) = t$. The symbols o, O, $\ll$ and $\asymp$ will be as usual (see [5]), and the implied constants may depend on A and δ.

2. A GENERAL TRANSFORMATION FORMULA

The next theorem is an analogue of Theorem 3.2 of Jutila [5]. It is more general than what would be necessary for the proof of Theorem 1, but we state if because it may also be of independent interest. The proof rests on Theorem 2 in Meurman [7] and on theorems on exponential integrals in Jutila [5]. Our result is left in a somewhat unfinished shape in order to dispense with the "Ramanujan-Petersson conjecture".

THEOREM 2. *Let* $2 \le M_1 < M_2 \le 2M_1$ *and define*

$D = D_\lambda = \{z \in \mathbb{C} : |z-x| < \lambda$ *for some* $x \in [M_1, M_2]\}$.

Let f *and* g *be holomorphic functions in* D *for some* λ *with* $M_1 << \lambda < M_1$. *Suppose*

(2.1) $g(z) << G$ *for any* $z \in D$,

(2.2) $f(x)$ *is real for any* $x \in [M_1, M_2]$,

(2.3) $f'(z) << |r|$ *for any* $z \in D$,

(2.4) $f''(x) >> |r| M_1^{-1}$ *for any* $x \in [M_1, M_2]$.

Suppose

(2.5) $f'(M(r)) = r$

for a certain number $M(r) \in (M_1, M_2)$ *and write*

(2.6) $M_j = M(r) + (-1)^j m_j$, $(j = 1, 2)$.

Suppose

(2.7) $\max(|hk|, (M_1/|r|)^{1/2}) M_1^{\delta} << m_1 << M_1^{1-\delta}$, $m_1 \asymp m_2$,

(2.8) $k\kappa \le \min(1, \kappa) M_1^{1/2}$,

(2.9) $0 < U \le (1/2)\min(m_1, m_2)$.

Define

(2.10) $P(v,z) = (v^2 + z^2)^{1/2} - v \operatorname{arsinh}(v/z) - \pi/4$,

(2.11) $$p_{j,n}(z) = f(z) - rz - (-1)^j \frac{1}{2\pi} P(2\kappa, 4\pi\sqrt{nz}/k),$$

(2.12) $$n(x) = k^2 x((f'(x) - r)^2 - (\frac{\kappa}{2\pi x})^2),$$

$$n_j(u) = n(M_j - (-1)^j u),\ n_j = n(M_j),$$

and let $x_{j,n}$ *be the (unique) zero of* $p'_{j,n}(x)$ *in the interval* (M_1, M_2) *when* $n < n_j$. *Then*

(2.13) $$U^{-1} \int_0^U \sum_{M_1+u\le m\le M_2-u} \rho(m)g(m)e(f(m))du =$$

$$\frac{i}{\sqrt{2k}} \sum_{j=1}^{2} (-1)^{j+1} \frac{1}{U} \int_0^U \sum_{n<n_j(u)} \rho(n)g(x_{j,n}) \cdot$$

$$\left(nx_{j,n} + (\frac{k\kappa}{2\pi})^2\right)^{-1/4} \left(p''_{j,n}(x_{j,n})\right)^{-1/2} \cdot$$

$$\cdot\ e(p_{j,n}(x_{j,n}) - \bar{r}n + 1/8)du +$$

$$+ O(G(C_\psi |h| km_1)^{1/2}) + O(U^{-1} G C_\psi^{1/2} k^{3/2} (hm_1)^{-1/2} M_1) +$$

$$+ O(G(|h|km_1)^{1/2} \sum_{j=1}^{2} U^{-1} \int_0^U \sum_{n\le 2n_1+2n_2} |\rho(n)|(|n-n_j(u)| +$$

$$+ |h|^{3/2} k^{1/2} m_1 M_1^{-1/2})^{-1} du).$$

If

(2.14) $\quad 0 < U \ll (M_1/|r|)^{1/2}$

then $n_j(u)$ *may be replaced by* n_j *in the explicit term and in the last* 0*-term.*

3. PROOF OF THEOREM 2

Suppose, for definiteness, that $r > 0$, and thus $h > 0$. The proof is similar for $r < 0$.

Let $q = k\kappa/2\pi$. It is convenient to have the next few properties at disposal. Since f is holomorphic in D we have by (2.3) and (2.4)

(3.1) $\quad f''(x) \asymp r/M_1$ if $M_1 \le x \le M_2$.

Hence and by (2.5) - (2.8) n(x) defined in (2.12) satisfies

(3.2) $\quad n(x) \asymp (hm_1)^2/M_1$ if $M_1 \le x \le M_2$ and $|x-M(r)| \gg m_1$.

Consider (2.10) and (2.11). We have $\frac{\partial}{\partial z} P(v,z) = \sqrt{1 + (v/z)^2}$ whence

(3.3) $\quad p'_{j,n}(z) = f'(z) - r - (-1)^j \frac{1}{kz} (nz + q^2)^{1/2}$

and

$$p''_{j,n}(z) = f''(z) + (-1)^j, k^{-1} z^{-2} (nz + q^2)^{-1/2} (nz/2 + q^2) \quad (3.4)$$

Together with (3.1), (3.2) and (2.7) this yields

$$p''_{j,n}(x) \asymp r/M_1 \quad \text{if} \quad M_1 \le x \le M_2 \quad \text{and} \quad n \ll n_j \quad (3.5)$$

since by (2.8) we have

$$|nz + q^2| \asymp nM_1 \quad \text{if} \quad z \in D \quad (3.6)$$

By (3.3), (2.4), (2.5) and (2.12) we have

$$\left(\frac{\partial}{\partial y} p_{j,n(x)}(y)\right)_{y=x} = 0 \quad \text{if} \quad (-1)^j (x - M(r)) \ge 0 \quad (3.7)$$

$$\text{and} \quad M_1 \le x \le M_2 .$$

After these preliminaries we may go into the proof of Theorem 2. Let $a_1 = M_1 + u$, $a_2 = M_2 - u$ and

$$S = \frac{1}{U} \int_0^U \sum_{a_1 \le m \le a_2} \rho(m) g(m) e(f(m)) du , \quad (3.8)$$

i.e. the expression on the left-hand side of (2.13).

Using the identities $e(f(m)) = e(f(m) - rm)e(rm)$ and $J_{iv}(z) = \frac{1}{2}(H^{(1)}_{iv}(z) + H^{(2)}_{iv}(z))$ we obtain by Theorem 2 in [7]

$$S = S' + \frac{1}{U}\int_0^U 4k^{-1}(\cosh \pi\kappa) \sum_{n=1}^{\infty} \rho(-n)e(\bar{r}n)V_n du ,$$

where

$$(3.9) \qquad S' = \frac{\pi i}{2k \sinh \pi\kappa} \sum_{n=1}^{\infty} \rho(n)e(-\bar{r}n) \frac{1}{U}\int_0^U \sum_{j=1}^{2} (V^+_{n,j} - V^-_{n,j})du ,$$

$$(3.10) \qquad V^{\pm}_{n,j} = \int_{a_1}^{a_2} g(x)H^{(j)}_{\pm 2i\kappa}(4\pi\sqrt{nx}/k)e(f(x) - rx)dx$$

and

$$V_n = \int_{a_1}^{a_2} g(x)K_{2i\kappa}(4\pi\sqrt{nx}/k)e(f(x) - rx)dx .$$

By bounded convergence it was admissible to integrate term-by-term.

Consider V_n. By (2.1), (2.2), (2.8) and since $K_{2i\kappa}(y) \ll y^{-1/2}\exp(\pi\kappa - y)$, when $y > 0$, we have

$$V_n << Gk^2n^{-1}b_1^{1/2}\, e^{\pi\kappa - b_1} << GM_1b_1^{-1}\, e^{\pi\kappa - b_1} ,$$

where $b_1 = 4\pi\sqrt{na_1}/k >> 1$. By (1.1) and (2.8) this shows that $S - S' << \sqrt{C_\psi}Gk$. By (2.7) this is absorbed by the first 0-term in (2.13). Therefore it remains to consider S' as defined in (3.9) and (3.10).

By [8], §§8.6, 8.61, we have (see (2.10))

LEMMA 1. *Assume* v *is real,* Re(z) > 0 *and define* $h_v^{(j)}(z)$ *via*

$$H_{iv}^{(j)}(z) = \sqrt{2/\pi}(z^2 + v^2)^{-1/4}$$

$$\exp((-1)^{j-1}(\frac{\pi v}{2} + iP(v,z)))(1 + h_v^{(j)}(z)) .$$

Then $h_v^{(j)}(z)$ *is analytic in* z *and an even function of* v, *and for* $|v/z| \le 1/2$ *we have* $h_v^{(j)}(z) << |z|^{-1}$.

By Lemma 1, (3.10), (2.8) and (2.11)

$$(3.11) \qquad V_{n,j}^{\pm} = \frac{1}{\pi\sqrt{2}} k^{1/2} n^{-1/4} \exp(\pm(-1)^{j+1}\pi\kappa) T_{n,j} ,$$

where

$$T_{n,j} = \int_{a_1}^{a_2} g(x)(x + q^2/n)^{-1/4}$$

$$(1 + h_{2\kappa}^{(j)}(4\pi\sqrt{nx}/k))e(p_{j,n}(x))dx .$$

CASE 1. Assume $n \le 2n_j$. We shall evaluate $T_{n,j}$ by Theorem 2.1 (due to Atkinson) in [5] with $\mu(x) = \lambda/2$, $\alpha = -r$, $G(x) = GM_1^{-1/4}$, $F(x) = rM_1$ and $x_o = x_{j,n}$.

It is easy to verify the conditions of the theorem by our assumptions and the formulae at the beginning of this section.

We prove a lemma before writing down the expression for $T_{n,j}$.

LEMMA 2. *Let* $n \le 2n_j$ *and* $0 \le u < \min(m_1, m_2)$. *Then the function* $p'_{j,n}$ *has a zero (denoted by* $x_{j,n}$*) in the interval* $(M_1 + u, M_2 - u)$ *if and only if* $n < n(a_j)$. *The zero is unique and* $x_{1,n} < M(r) < x_{2,n}$.

PROOF. By (3.3) $n < n(a_j)$ if and only if $(-1)^j p'_{j,n}(a_j) > (-1)^j p'_{j,n(a_j)}(a_j)$. The right-hand side is 0 by (3.7) and (2.6). On the other hand $(-1)^j p'_{j,n}(M(r)) < 0$ by (3.3) and (2.5). The lemma now follows by (3.5).

Now we have

$$(3.12)\quad T_{n,j} = g(x_{j,n})(x_{j,n} + q^2/n)^{-1/4}(p''_{j,n}(x_{j,n}))^{-1/2} \cdot$$

$$\cdot (1 + h_{2\kappa}^{(j)}(4\pi\sqrt{nx_{j,n}}/k))e(p_{j,n}(x_{j,n}) + 1/8) +$$

$$+ O(GM_1^{-1/4} m_1 e^{-ArM_1}) + O(GM_1^{-3/4} r^{-3/2})$$

$$+ O(E_o(a_1) + E_o(a_2)) ,$$

where the explict term on the right is to be omitted when $n(a_j) \le n \le 2n_j$ and

$$E_o(a_\nu) = GM_1^{-1/4}(|p'_{j,n}(a_\nu)| + (p''_{j,n}(a_\nu))^{1/2})^{-1}.$$

By Lemma 1 and (2.8) $h_{2\kappa}^{(j)}(...)$ in (3.12) is $\ll k(nM_1)^{-1/2}$. If we omit this we get by (2.1), (3.6) and (3.5) an error

$$0(GkM_1^{-1/4}r^{-1/2}n^{-1/2}) ,$$

and by (2.7) and (3.2) this absorbes the first two 0-terms in (3.12).

Consider $E_o(a_\nu)$. By (3.7), (3.3) and (3.6) we have

$$(3.13)\quad |p'_{j,n}(a_\nu)| = |p'_{j,n}(a_\nu) - p'_{\nu,n(a_\nu)}(a_\nu)| \gg$$

$$\gg k^{-1}(M_1 n(a_\nu))^{-1/2}|n - n(a_\nu)| .$$

Together with (3.2) and (3.5) this yields

$$(3.14)\quad E_o(a_\nu) \ll GM_1^{-1/4}hkm_1(|n - n(a_\nu)| +$$

$$+ h^{3/2}k^{1/2}m_1M_1^{-1/2})^{-1}.$$

Assume now for a moment that (2.14) is satisfied. By (2.7) this clearly implies (2.9). Then by (3.5) and (2.7)

$$p'_{j,n}(a_\nu) - p'_{j,n}(M_\nu) << UrM_1^{-1} <<$$

$$<< (r/M_1)^{1/2} \asymp (p''_{j,n}(a_\nu))^{1/2} .$$

On the other hand we get with $u = 0$ in (3.13)

$$|p'_{j,n}(M_\nu)| >> k^{-1}(M_1 n_1)^{-1/2}|n - n_\nu| ,$$

so that in this case (3.14) is valid if $n(a_\nu)$ is replaced by n_ν.

Let us still assume (2.14). If $n(a_j) \le n < n_j$ then $|x_{j,n} - M_j| \le U$ by Lemma 2. Then $x_{j,n} - a_j << U$, whence we obtain, like before, $p'_{j,n}(a_j) << \sqrt{p''_{j,n}(a_j)}$. Then the explicit term in (3.12) is $<< E_o(a_j)$ so that it may be retained for these values of n.

With these observations in mind and by (1.1), (3.11), (3.2) and (2.7) we find that

$$(3.15)\quad \frac{\pi i}{2k \sinh \pi\kappa} \frac{1}{U} \int_0^U \sum_{j=1}^{2} \sum_{n \le 2n_j} \rho(n) e(-\bar{r}n)(V^+_{n,j} - V^-_{n,j})du$$

equals the explicit term plus the first and third error terms in (2.13). Moreover the assertion depending on (2.14) holds.

CASE 2. Assume $n > 2n_j$. We shall estimate

$$T^*_{n,j} = \frac{1}{U}\int_0^U T_{n,j}\,du$$

by Theorem 2.3 in [5] with m_1 in place of μ, $k^{-1}M_1^{-1/2}n^{1/2}$ in place of M and $GM_1^{-1/4}$ in place of G.

First we have to check that

(3.16) $p'_{j,n}(z) \ll M$ for $z \in D_{m_1}$

and

(3.17) $|p'_{j,n}(x)| \gg M$ for $x \in [M_1, M_2]$.

The other conditions of the theorem are clearly satisfied.

By (2.5) and (2.3) we have $f'(z) - r \ll m_1|r|/M_1$ for $z \in D_{m_1}$. Together with (3.3), (3.6) and (3.2) this proves (3.16).

By (3.5) $p'_{j,n_j}(x)$ is increasing on $[M_1, M_2]$. Hence using (3.7) with $x = M_j$ we get $(-1)^j p'_{j,n_j}(x) \le 0$. By (3.3)

$$|p'_{j,n}(x)| = |p'_{j,n}(x) - p'_{j,n_j}(x) + p'_{j,n_j}(x)| =$$

$$= |\frac{1}{kx}((nx+q^2)^{1/2} - (n_jx+q^2)^{1/2}) -$$

$$- (-1)^j p'_{j,n_j}(x)|,$$

so that (3.17) follows, since $n > 2n_j$.

We obtain, using (2.7) and (3.2),

$$T^*_{n,j} << U^{-1} G M_1^{3/4} k^2 n^{-1} .$$

Hence and by (1.1), (3.11) and (3.2) we find that

$$(3.18) \quad \frac{\pi i}{2k \sinh \pi\kappa} \sum_{j=1}^{2} \sum_{n>2n_j} \rho(n) e(-\bar{r}n) \frac{1}{U} \int_0^U (V^+_{n,j} - V^-_{n,j}) du$$

gives rise to the second 0-term in (2.13). Since the series above converges the sum of (3.15) and (3.18) equals $\sum_j \sum_n = \sum_n \sum_j = S'$ (see (3.9)) and the proof is complete.

4. TRANSFORMATION OF A SHORT DIRICHLET POLYNOMIAL

The next theorem follows by Theorem 2. It is an analogue of Theorem 4.2 of Jutila [5]. For simplicity we assume t is positive.

THEOREM 3. *Let* $t >> 1$ *and*

$$(4.1) \quad 2 \le M_1 < \frac{t}{2\pi r} < M_2 \le 2M_1 .$$

Writing

$$M_j = \frac{t}{2\pi r} + (-1)^j m_j$$

assume

$$(4.2) \quad t^{\delta}\max(hk, t^{1/2}r^{-1}) \ll m_1 \ll M_1^{1-\delta},\ m_1 \asymp m_2,$$

$$(4.3) \quad k\kappa \le \min(1,\kappa)M_1^{1/2},$$

$$(4.4) \quad 0 < U \le \frac{1}{2}\min(m_1, m_2).$$

Define

$$(4.5) \quad N_j(u) = \frac{h^2(m_j - u)^2}{M_j - (-1)^j u},\ N_j = N_j(0),$$

$$(4.6) \quad F(x) = F(x,t,\kappa) = -(2xt + x^2 + \kappa^2)^{1/2} - \pi/4 -$$

$$- 2(t+\kappa)\operatorname{arsinh}\left(\frac{1}{2}\frac{x+t}{\sqrt{t^2 - \kappa^2}} - \frac{1}{2}\right)^{1/2} +$$

$$+ 2\kappa \operatorname{arsinh}\frac{x+\kappa}{\sqrt{2x(t-\kappa)}}$$

and let $\chi(s) = \zeta(s)/\zeta(1-s)$. *Then*

$$(4.7) \quad U^{-1}\int_0^U \sum_{M_1+u\le n\le M_2-u} \rho(n)n^{-1/2-it}\,du =$$

$$\left(\frac{2}{\pi}(hkt)^{-1/4}r^{it}\left(\chi\left(\tfrac{1}{2}+i(t+\kappa)\right)\chi\left(\tfrac{1}{2}+i(t-\kappa)\right)\right)^{1/2} \sum_{j=1}^{2} U^{-1}\right.$$

$$\cdot \int_0^U \sum_{n<N_j(u)} \rho(n) e(n(\bar{r} - \frac{1}{2hk})) \, n^{-1/4}(1+\frac{\pi n}{2hkt})^{-1/4} \, e^{(-1)^j iF(\pi n/hk)} du$$

$$+ O(C_\psi^{1/2} h m_1^{1/2} t^{-1/2}) + O(U^{-1} C_\psi^{1/2} h^{-1} k^2 m_1^{-1/2} t^{1/2})$$

$$+ O(h m_1^{1/2} t^{-1/2} \sum_{j=1}^{2} U^{-1} \int_0^U \sum_{n \le 3N_1+3N_2} |\rho(n)| (|n-N_j(u)| + h^2 m_1 t^{-1/2})^{-1} du),$$

where the square root involving χ *equals* $\chi(\frac{1}{2} + it)$, *when* $\kappa = 0$, *and is a continuous function of* $\kappa \ge 0$. *If* $0 < U \ll$ $\ll t^{1/2}/r$ *then* $N_j(u)$ *may be replaced by* N_j *in the explicit term and in the last* O*-term.*

5. PROOF OF THEOREM 3

We apply Theorem 2 with $-r$ in place of r, $\lambda = M_1/2$,

$$(5.1) \qquad f(z) = -\frac{t}{2\pi} \log z \, ,$$

$$(5.2) \qquad g(z) = z^{-1/2} \, ,$$

$$(5.3) \qquad G = (h/kt)^{1/2} \, .$$

Then the left-hand sides of (2.13) and (4.7) are equal and it is easy to verify all the assumptions.

By (4.3) $n_j(u)$ in (2.12) and $N_j(u)$ in (4.5) satisfy

(5.4) $\quad N_j(u) - n_j(u) \ll 1 ,$

when $0 \le u \le U$. Hence and by (4.2) and (5.3) the 0-terms in Theorem 2 give rise to those in Theorem 3.

Consider the explicit term. Write, for brevity,

$$v = \frac{kt}{2\pi} , \quad q = \frac{k\kappa}{2\pi} , \quad d = \frac{n}{2h} , \quad x = x_{j,n}.$$

First we need explicit expressions for x and 1/x. By (3.3) (5.1) and the defintion of x we have (recall that we replaced r by -r)

(5.5) $\quad (nx + q^2)^{1/2} = (-1)^j(hx - v) .$

We solve for x and obtain

(5.6) $\quad x = h^{-1}(d + v + (-1)^j(2dv + d^2 + q^2)^{1/2})$

whence

(5.7) $\quad x^{-1} = h(v^2 - q^2)^{-1}(d + v - (-1)^j(2dv + d^2 + q^2)^{1/2}).$

By (3.4) and (5.1) we have

$$x(nx + q^2)^{1/2} p''_{j,n}(x) = (kx)^{-1}(v(nx + q^2)^{1/2} + (-1)^j(nx/2 + q^2)) .$$

By (5.5) this is $(-1)^j k^{-1}(hv + n/2 + x^{-1}(q^2 - v^2))$. Hence and by (5.2) and (5.7)

$$g(x)(nx + q^2)^{-1/4}(p''_{j,n}(x))^{-1/2} =$$

$$= k^{1/2}(hnv + (hd)^2 + (hq)^2)^{-1/4} =$$

$$= k^{1/2}(hnv)^{-1/4}(1 + d/2v)^{-1/4} +$$

$$+ O(r^{3/4}(nt)^{-5/4}\, q^2).$$

The 0-term here may be omitted, since by (1.1) it contributes $\ll c_\psi^{1/2}(hk)^{3/4}t^{-5/4}\kappa^2$ and by (4.2) and (4.3) this is absorbed by the first 0-term in (4.7).

We proceed to evaluate $p_{j,n}(x)$. Write, for brevity,

$$a = (d + v)^2, \quad b = v^2 - q^2 .$$

Then (5.6) and (5.7) may be rewritten as

$$hx = \sqrt{a} + (-1)^j\sqrt{a-b},\ (hx)^{-1} = b^{-1}(\sqrt{a} - (-1)^j\sqrt{a-b}) ,$$

so that

$$(hx/\sqrt{b})^{(-1)^j} = \sqrt{a/b} + \sqrt{a/b - 1} =$$

$$= (((\sqrt{a/b} - 1)/2)^{1/2} + ((\sqrt{a/b} - 1)/2 + 1)^{1/2})^2.$$

Hence

$$\log x = (-1)^j\, 2\, \operatorname{arsinh}(\tfrac{1}{2}\sqrt{a/b} - \tfrac{1}{2})^{1/2} + \log\sqrt{b} - \log h. \tag{5.8}$$

Next we evaluate $(-1)^j \operatorname{arsinh}(q/\sqrt{nx})$. By squaring and applying (5.6) and (5.5) we easily find (note: $q \le v$)

$$(q^2 + nx)^{1/2} + (-1)^j q = ((d + q)^2 + 2d(v - q))^{1/2} + (-1)^j (d + q).$$

Taking logarithms of each side and using then the identity $\log(\sqrt{y^2 + 1} + (-1)^j y) = (-1)^j \operatorname{arsinh} y$ we obtain

$$(-1)^j \operatorname{arsinh}(q/\sqrt{nx}) + \frac{1}{2} \log nx =$$

$$= (-1)^j \operatorname{arsinh}((d + q)/\sqrt{2d(v - q)}) + \frac{1}{2} \log(2d(v - q)).$$

Hence and by (2.10), (2.11), (5.1), (5.5), (5.6) and (5.8) we have

$$p_{j,n}(x) = k^{-1}(T_1 + T_2),$$

where

$$T_1 = v - v \log\sqrt{t^2 - \kappa^2} - q \log\sqrt{(t + \kappa)/(t - \kappa)}$$

and

$$T_2 = -d + (-1)^j k/8 + v \log 2\pi h/k - (-1)^j (2dv + d^2 + q^2)^{1/2} -$$

$$- 2(-1)^j (v + q) \operatorname{arsinh}(\tfrac{1}{2}(d + v)/\sqrt{v^2 - q^2} - \tfrac{1}{2})^{1/2} +$$

$$+ 2q(-1)^j \operatorname{arsinh}((d + q)/\sqrt{2d(v - q)}) .$$

By (4.6)

$$k^{-1} T_2 = (-1)^j \frac{1}{2\pi} F(\tfrac{\pi n}{hk}) + \frac{t}{2\pi} \log(2\pi r) - \frac{n}{2hk} + \frac{1}{4}(-1)^j .$$

Let $K = \chi(\frac{1}{2} + i(t+\kappa))\chi(\frac{1}{2} + i(t-\kappa))$. By Stirling's formula (or [4], (1.25))

$$K = i(2\pi)^{2it}e(2k^{-1}T_1)(1 + O(1/t)) .$$

Hence

$$e(k^{-1}T_1) = e^{-i\pi/4}(2\pi)^{-it}K^{1/2} + O(1/t) ,$$

where $K^{1/2} = \chi(\frac{1}{2} + it)$, when $\kappa = 0$ and $K^{1/2}$ is a continuous function of $\kappa \geq 0$. The O-term here contributes $\ll C_\Psi^{1/2}h^2k^{-1}t^{-2}m_1^{3/2}$ by (1.1) and (4.5). This is absorbed by the first O-term in (4.7), since $m_1 \ll t/r$.

Putting these facts together almost completes the proof. It only remains to replace $n_j(u)$ by $N_j(u)$ in the explicit term. By (5.4) and (4.5) the arising error can be absorbed by the third O-term in (4.7).

6. PROOF OF THEOREM 1

Consider $L(s)$ which was defined in Section 1. Let $p = 0$ if ρ is even and $p = 1$ if ρ is odd. Then $L(s) = \eta_p(s)L(1-s)$, where

$$(6.1) \qquad \eta_p(s) = \chi(s+i\kappa)\chi(s-i\kappa)(-\cot\tfrac{\pi}{2}(s+i\kappa)\cot\tfrac{\pi}{2}(s-i\kappa))^p$$

and $\chi(s) = \zeta(s)/\zeta(1-s)$. $L(s)$ is entire and $\eta_p(s)$ has simple poles at $2n + 1 + p \pm i\kappa$, where $n = 0,1,2, \ldots$. These facts follow by Section 2 in [7], or in the case $p = 0$, by [1].

Let $s = \sigma + it$. By (4.3) in [7] we have $L(s) \ll_\kappa (|t| + 1)^A$, when $\sigma \ll 1$.

We have $(2\pi)^s\Gamma(1-s)\Phi(\pi s/2) \ll \max(|s|^{1/2-\sigma}, 1)$ for for $\sigma \leq 1/2$, where $\Phi = \sin$ or $\Phi = \cos$. Hence and by (6.1) we have for $\sigma \leq 1/2$

$$\eta_p(s) \ll (\max(|s+i\kappa|,1)\max(|s-i\kappa|,1))^{1/2 - \sigma}.$$

Now using the reflection principle (see e.g. [4], 4.4) in combination with the above facts and (1.1) and (1.2) we find that Theorem 1 follows if we can prove

LEMMA 3. *For* $t \gg 1$, $\kappa \ll t^{1/3}$, $t^{2/3 + \delta} \leq N \ll t$, $s = \frac{1}{2} + it$ *and* $\delta > 0$ *we have*

$$\frac{1}{N}\int_N^{2N} \Big|\sum_M^{2M} \rho(n)n^{-s}\Big| dM \ll_\delta C_\psi^{1/2} t^{1/3 + \delta}.$$

(The case with $1 - s$ in place of s is similar.)

Let

$$S(M,2M) = \sum_{M\leq n\leq 2M} \rho(n)n^{-1/2 - it},$$

where $N \leq M \leq 2N$. Let $M_o = t^{2/3+\delta}$ and

$$K = (M/M_o)^{1/2}. \tag{6.2}$$

Denote by F_K the sequence of the reduced positive rationals $r = h/k$, where $1 \leq k \leq K$. For each r in F_K such that $r > 1/[K]$ let r_2, r and r_1 be consecutive elements in F_K such that $r_2 < r < r_1$. Let $\mu_j(r)$ be the mediant of r and r_j. Then

$$|r - \mu_j(r)| \asymp (kK)^{-1}. \tag{6.3}$$

Let

$$U = Mt^{-1/3} \tag{6.4}$$

and

$$M_j = t(2\pi\mu_j(r))^{-1} + (-1)^j U/2. \tag{6.5}$$

By (6.3) we have

$$r \asymp \mu_j(r). \tag{6.6}$$

Now subdivide the interval $[M,2M]$ by all the points $M_1 + u$, where r is in F_K and $0 \leq u \leq U$. (u is fixed.) The subintervals are of the form

$$[M_1 + u,\ M_2 + u - U] \cap [M,2M], \tag{6.7}$$

since $\mu_1(r_2) = \mu_2(r)$.

If (6.7) is non-empty then by (6.4) - (6.6) we have

(6.8) $\quad t \asymp Mr.$

Hence and by (6.2) we have

(6.9) $\quad hK \ll t^{1/3 - \delta}$

Hence and by (6.4) we have

(6.10) $\quad U \ll M(hK)^{-1}t^{-\delta}.$

Hence and by (6.2), (6.3), (6.5), (6.6) and (6.8) we have

(6.11) $\quad |M_j - \frac{t}{2\pi r}| \asymp M(hK)^{-1} \ll Mt^{-1/6 + \delta/2}.$

Denote by R the set of those r in F_K satisfying $M_1 \geq M$ and $M_2 \leq 2M$. If r belongs to R then (6.7) is $[M_1 + u, M_2 + u - U]$. Otherwise (6.11) shows that (6.7) is contained in

$$I(M) = [M, M + Mt^{-1/6 + \delta}] \cup [2M - Mt^{-1/6 + \delta}, 2M].$$

Then writing

(6.12) $\quad S' = \sum_{r \in R} U^{-1} \int_0^U S(M_1 + u, M_2 - u)du$

we have

$$S(M,2M) - S' \ll M^{-1/2} \sum_{n\in I(M)} |\rho(n)|.$$

Now

$$N^{-1}\int_N^{2N} M^{-1/2} \sum_{n\in I(M)} |\rho(n)|dM \ll N^{-3/2} \sum_N^{4N} |\rho(n)| \int_N^{2N} dM \ll$$

$$\ll C_\psi^{1/2} t^{1/3 + \delta}$$

by (1.1). Hence Lemma 3 follows if we can prove

(6.13) $S' \ll C_\psi^{1/2} t^{1/3 + 2\delta}$

for $\kappa \ll t^{1/3}$ and $M_o \le M \ll t$.

The next step is to apply Theorem 3 to (6.12). Recall that now we have $M_j \asymp M$. Let

$$m_j = (-1)^j (M_j - \frac{t}{2\pi r}).$$

This is positive by (6.5), and by (6.11) we have

(6.14) $m_j \asymp M(hK)^{-1}$.

By (6.9) we have $hkt^\delta \ll m_1$, since $M \ge M_o$. By (6.2) we have $t^{1/2+\delta} \ll rm_1$. On the other hand $m_1 \ll M_1^{1-\delta}$ by (6.11). Hence (4.1) and (4.2) are satisfied, and (4.3) follows by

(6.2) and the assumption $\kappa \ll M_o^{1/2} t^{-\delta/2}$. Finally (4.4) is clearly satisfied by (6.10).

Consider (4.5). By (6.2) and (6.14) we have for $0 \le u \le U$

(6.15) $\quad N_j(u) \asymp M_o$.

Denote by $O(E_1)$, $O(E_2)$ and $O(E_3)$ the error terms in Theorem 3. By (6.14) and (6.8) we have $E_1 \ll \sqrt{C_\psi}$. Since $U \ll m_1$, we have $E_2 \ll E_1$ by (6.8) and (6.4). By (6.14), (6.15) and (6.8) we have

$$E_3 \ll \sum_{j=1}^{2} \sum_{n \le AM_o} |\rho(n)| U^{-1} \int_0^U (|n - N_j(u)| + t^{1/2} k K^{-1})^{-1} du .$$

By (4.5), (4.2) and (4.4) we have $|dN_j(u)/du| \asymp h^2 m_1 / M_1 \asymp h/K$. Therefore the integral above is $\ll Kh^{-1} t^{\delta}$. Hence and by (1.1), (6.4) and (6.8) we have $E_3 \ll \sqrt{C_\psi} t^{2\delta} K/k$.

By (6.8) and (6.2) we have

$$\sum_{r \in R} Kk^{-1} \ll t^{1/3 - \delta}.$$

Therefore the contribution of the terms $O(E_m)$ to S' is $\ll \sqrt{C_\psi} t^{1/3 + \delta}$.

Finally consider the explicit term in Theorem 3. By (6.15) we may remove the factor $(1 + \pi n/2hkt)^{-1/4}$ with a negligible error. The contribution of the remaining

expression to S' is

$$\ll U^{-1}t^{-1/4} \int_0^U \sum_{j=1}^{2} |S''|du ,$$

where

$$S'' = \sum_{r\in R} (hk)^{-1/4} r^{it} \sum_{n<N_j(u)} \rho(n)e(na_r)n^{-1/4}e^{(-1)^j i}\, F(\pi n/hk) ,$$

and a_r depends only on r. Here we invert the order of summations, use Cauchy's inequality, (6.15) and (1.1) to obtain

$$S'' \ll C_\psi^{1/2} M_o^{1/4} (S''')^{1/2} ,$$

where

$$S''' = \sum_{n\leq AM_o} \left| \sum_{\substack{r\in R \\ n<N_j(u)}} (hk)^{-1/4} r^{it} e(na_r) e^{(-1)^j iF(\pi n/hk)} \right|^2 .$$

Restricting the summations to intervals $X \leq n < 2X$ and $K_o \leq k < 2K_o$, writing out the square as a double sum, inverting the order of the summations and using

(6.16) $\quad hk \asymp rk^2 \asymp tM^{-1}K_o^2$

(see (6.8)) we obtain

$$S''' \ll \log^3 t \max_{\substack{1\le X\le AM_o \\ 1\le K_o\le K}} t^{-1/2} M^{1/2} K_o^{-1} \sum_{\substack{r,r'\in R \\ K_o\le\{k,k'\}<2K_o}} |s(r,r')|,$$

where $r' = h'/k'$,

$$s(r,r') = \sum_{\substack{X\le n<2X \\ n<\min(N_j(u),N_j'(u))}} e(f(n)),$$

$$f(x) = x(a_r - a_{r'}) + \frac{1}{2\pi}(-1)^j (F(\pi x/hk) - F(\pi x/h'k'))$$

and $N_j'(u)$ depends on r' in the same way as $N_j(u)$ on r.

We shall evaluate $f''(x)$. By (4.6) we have

$$\frac{d}{dx} F(\pi x/y) = -x^{-1}((\pi x/y)^2 + 2\pi tx/y + \kappa^2)^{1/2} .$$

Hence

$$-\frac{d^2}{dx^2} F(\pi x/y) = x^{-2}(\pi tx/y + \kappa^2)((\pi x/y)^2 + 2\pi tx/y + \kappa^2)^{-1/2} .$$

Hence

$$\frac{d}{dy}\frac{d^2}{dx^2} F(\pi x/y) = \pi^2(\kappa^2 - t^2)((\pi x)^2 + 2\pi txy + (\kappa y)^2)^{-3/2} .$$

Now by (6.16) and since $K^{\kappa} \ll \sqrt{M}$ we have for $x \asymp X$

$$|f''(x)| \asymp |hk - h'k'| t^{-1} X^{-3/2} M^{3/2} K_o^{-3}.$$

Therefore we obtain exactly as in Section 4.2 of [5]

$$S''' \ll t^{5/6 + 3\delta},$$

which in combination with the previous estimates yields (6.13). This completes the proof of Theorem 1.

REFERENCES

[1] C. EPSTEIN, J.L. HAFNER and P. SARNAK, Zeros of L-functions attached to Maass forms, *Math. Z.* 190 (1985), 113-128.

[2] A. GOOD, The square mean of Dirichlet series associated with cusp forms, *Mathematika* 29 (1982), 278-295.

[3] M.N. HUXLEY, Introduction to Kloostermania, *Elementary and analytic theory of numbers, Banach Cent. Pub.* 17 (1985), 217-306.

[4] A. IVIĆ, The Riemann zeta-function. *John Wiley & Sons*, New York, 1985.

[5] M. JUTILA, Lectures on a method in the theory of exponential sums. *Tata Institute of Fundamental Research, Lectures on mathematics and physics 80*, Bombay, 1987.

[6] H. MAASS, Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* 121 (1949), 141-183.

[7] T. MEURMAN, On exponential sums involving the Fourier coefficients of Maass wave forms, J. reine angew. Math. 384 (1988), 192-207.

[8] G.N. WATSON, A treatise on the theory of Bessel functions, 2nd ed., Cambridge Univ. Press, Cambridge, 1944.

TOM MEURMAN
University of Turku
Department of Mathematics
SF-20500 Turku
Finland

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

q-ADIC SPECTRAL ANALYSIS OF ARITHMETIC SEQUENCES

MOSSÉ, B.

We present in this paper a way of analysing arithmetic sequences. This topic, on which also J. Coquet worked [2], is close to the classical spectral analysis, but depends on the choice of a basis q. It permits to calculate easier spectral measures for sequences depending on a certain way on this basis.

Let q be an integer greater than 2.
We define the q-adic addition of natural integers as follow:

if $n = \sum_{r\geq 0} n_r q^r$, $n_r \in \{0,\ldots,q-1\}$

and

$m = \sum_{r\geq 0} m_r q^r$, $m_r \in \{0,\ldots,q-1\}$, then

$n \oplus m = \sum_{r\geq 0} e_r q^r$, where e_r is the remainder of $n_r + m_r$ modulo q.

With this operation, $\mathbb{N}$ is a group G_q isomorphic to $(\mathbb{Z}/q\mathbb{Z}[X],+)$. The dual of G_q is a group isomorphic to $\mathbb{Z}/q\mathbb{Z}^{\mathbb{N}}$. The characters of this dual are the Walsh characters [6] given by

$$w_n(t) = \prod_{r\geq 0} \exp(2i\pi\, t_r\, n_r\, q^{-1}),$$

where $n \in \mathbb{N}, (n_r)_{r\in\mathbb{N}}$ is the sequence of the digits of n in base q, and $t \in G_q$ is identified with the sequence $(t_r)_{r\in\mathbb{N}}$

Let S_q be the set of sequences of complex numbers such that:

$$|u_n| = 1, \quad \text{for each } n \in \mathbb{N}, \quad u_0 = 1,$$

$$\lim_{N\to\infty} N^{-1} \sum_{n<N} u_n \oplus t\, \overline{u_n}$$

exists for each integer t.

We denote this limit by $\gamma^u(t)$. If u is an element of S_q, γ^u is called the Walsh correlation of u. γ^u is G_q-positive definite, and from the Bochner-Herglotz theorem we deduce that γ^u is the Fourier transform of a probability measure λ^u on the dual of G_q, called the Walsh

spectral measure of u. The following proposition specifies the discrete and the continuous components of λ^u:

PROPOSITION: 1) *Let* α *be an element of* $\hat{G}_q$; *then*

$$\overline{\lim_{N\to\infty}} N^{-1} \left| \sum_{n<N} u_n \overline{w_n(\alpha)} \right| \leq \lambda^u(\{\alpha\})^{1/2}.$$

2) λ^u *is continuous if and only if:*

$$\lim_{N\to\infty} N^{-1} \sum_{n<N} |\gamma^u(n)|^2 = 0.$$

We obtain a Van der Corput theorem:

THEOREM 1: *Let* u *be a sequence of real numbers. If the sequence* $(u(n \oplus k)-u(n))_{n\in\mathbb{N}}$ *is uniformly distributed modulo one for each integer* $k > 0$, *then* u *is also uniformly distributed modulo one.*

We now give some examples of calculations of Walsh spectral measures concerning q'*-multiplicative sequences. Let* q' *be an integer greater than* 2. *A sequence* u *of complex numbers is said* q'*-multiplicative if:*

$u_0 = 1$, and $u(a\, q'^{l} + b) = u(a\, q'^{l})\, u(b)$,

$\forall\, a, b, l \in \mathbb{N}$, $b < q'^{l}$.

THEOREM 2: *Let* u *be a* q'*-multiplicative sequence such that* $|u_n| = 1$. *Then* u *is an element of* S_q.

In that case, we can express γ^u using only finite

sums, but the general expression of γ^u is not very simple. So we give more details about two particular cases.

*$q = q'$

THEOREM 3:

1) If u *is a* q*-multiplicative sequence such that* $|u_n| = 1, \gamma^u$ *is also* q*-multiplicative.*

2) The Walsh spectral measure of u *is the infinite convolution product:*

$$\overset{*}{\underset{k\geq 0}{\Sigma}} \left[q^{-1} \sum_{j<q} \sum_{a<q} \gamma^u(a\, q^k)\ \overline{w_{aq^k}(\varepsilon_k^j)} \right] \delta_{\varepsilon_k^j},$$

where $\delta_{\varepsilon_k^j}$ *is the Dirac measure at the point* ε_k^j *of* $\hat{G}_q$ *defined by:*

$$\varepsilon_k^j(n) = \begin{cases} j & \text{if } n = k \\ 0 & \text{if } n \neq k \end{cases}.$$

This convolution product can be studied using the works of G. Brown and W. Moran [1]. *It is either discrete or continuous, and either singular or absolutely continuous with respect to the Haar measure on* $\hat{G}_q$.

For instance:

-1- *If* $u = \exp(2i\pi\alpha)$, $\alpha \in \mathbb{R}, \lambda^u$ *is discrete iff*

$$\alpha \in E_q = \{x \in \mathbb{Q};\ \exists k \in \mathbb{N},\ xq^k \in \mathbb{Z}\}.$$

-2- *If* $u = \exp(2i\pi \beta s_q(n))$, $\beta \in \mathbb{R}$, *where* $s_q(n)$ *is the sum of the digits of* n *in basis* q,

- *If* $\beta \equiv j/q \mod 1$, λ^u *is a Dirac measure,*
- *if* $q = 2$ and $\beta \equiv 1/4 \mod 1/2$, λ^u *is absolutely continuous,*
- *in the other cases,* λ^u *is singular continuous.*

$*(q',q) = 1$

THEOREM 4: *Let* u *be a* q'*-multiplicative sequence such that* $|u_n| = 1$.

1) *If the ordinary measure* Λ^u *of* u *is such that* $\Lambda^u(\{x\}) = 0$, $\forall x \in E_q$, *then* λ^u *is continuous.*
2) *If there is an element* α *of* E_q *such that* $\Lambda^u(\{x\}) = c>0$, *then* $\lambda^u = c\mu + (1-c)\mu'$, *where* μ *is a discrete measure and* μ' *is continuous.*

REFERENCES

[1] BROWN, G., MORAN, W., Coin tossing and powers of singular measures. *Math. Proc. Camb. Phil. Soc.* 77 (1975), pp 349-364.

[2] COQUET, J., Mesures spectrales de Walsh associées à certaines suites arithmétiques. *Ann. Inst. Fourier* 35, 2 (1985), pp. 1-12.

[3] MAUDUIT, C., MOSSÉ, B., Etude spectrale de la multiplication q-adique. To appear in Compositionnes Mathematica.

[4] MOSSÉ, B., q-adic spectral analysis of some arithmetic sequences. To appear in T.C.S.

[5] RAUZY, G., Propriétés statistiques de suites arithmétiques. P.U.F. (1976).

[6] WALSH, J.L., A closed set of normal orthogonal functions. *Amer. J. Math.* 55 (1923), pp. 5-24.

MOSSÉ, B.
C.N.R.S., UA 225,
Université d'Aix Marseille I,
Département de Mathématiques,
3, Place Victor Hugo, 13001 Marseille, F r a n c e

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

BENFORD'S LAW: THE LOGARITHMIC LAW OF FIRST DIGIT

KENJI NAGASAKA[1], SHIGERU KANEMITSU[2] and JAU-SHYONG SHIUE

0. INTRODUCTION

We are going to consider an infinite sequence of integers which we denote by $a = \{a_n\}_{n=1,2,\cdots}$. We write the number of a_n with $1 \le n \le N$ whose first digit begins with k or less than k by $A_N(a;k)$. Then we say that the sequence $a = \{a_n\}$ obeys Benford's law if, for every k, $k = 1,2,\cdots,9$,

$$\lim_{N\to\infty} \frac{A_N(a;k)}{N} = \log_{10}(k+1). \tag{0.1}$$

It turns out empirically that more numbers begin with one. Indeed, it comes up in all kinds of real data. Once we wrote down a collection of mathematical and

physical constants appeared in [1], and counted the number of appearances of 1 as first significant digits. Then its proportion was quite near to 301.

In this note we shall give, in Section 1, our fundamental tool from the theory of uniform distribution and explain how this can be applied to the powers of 2. Hence you will see the efficiency and the limit of our method.

In Section 2, we shall expose our results on linear recurrence integer sequences. Our results are almost the final one stated in terms of the roots of the characteristic equations of linear recurrence relations.

Then we shall consider the sequence of denominators of the n-th convergents in the simple continued fractions of real numbers. As a direct application of our results in this Section, we remark that Benford's law holds for the sequence of denominators of the n-th convergents of quadratic irrationals. We mention that this result is also proved by H. Jager and P. Liardet in [7].

In the final Section, we shall consider slowly increasing sequences of integers. In order to treat these integer sequences, we need other densities, such as, Banach limit, Dirichlet density or Murata's density other than natural density. We shall show that Benford's law holds for the sequence of primes in the sense of

Murata's density. We shall also give concluding remarks which include open problems on Benford's law.

1. FUNDAMENTAL TOOL FROM THE THEORY OF UNIFORM DISTRIBUTION

Let us consider the sequence of powers of 2, that is

$$a_n = 2^n. \tag{1.1}$$

A necessary and sufficient condition for $a_n = 2^n$ to begin with 1, is that the following inequalities hold for some nonnegative integer m:

$$1 \times 10^m \leq 2^n < 2 \times 10^m. \tag{1.2}$$

Taking the logarithms of the inequalities (1.2), we have:

$$m \leq n \times \log 2 < \log 2 + m. \tag{1.3}$$

We fix the base of the logarithms to be 10 unless otherwise specified. From an old but important result of the theory of uniform distribution, we know that the sequence $\{n \cdot \theta\}_{n=1,2,\ldots}$ is uniformly distributed mod 1, if θ is irrational. Since $\log 2$ is irrational (even transcendental),

the sequence $\{n \cdot \log 2\}$ is uniformly distributed mod 1. This signifies that the number of a_n with $1 \le n \le N$ for which the inequalities (1.3) hold is approximately $N \cdot \log 2$, and letting N tend to infinity, we obtain:

$$\lim_{N\to\infty} \frac{A_N(2^n;\ 1)}{N} = \log 2. \tag{1.4}$$

Let us count the number of occurences of 2^n with $1 \le n \le N$ whose first digits are k, $k = 1,2,\ldots,9$, that is, the following inequalities hold:

$$\log k + m \le n \log 2 < \log (k+1) + m, \tag{1.5}$$

for some nonnegative integer m. Uniform distribution property of $\{n \log 2\}$ assures that the limiting formula (0.1) holds for every k for $a = \{2^n\}_{n=1,2,\ldots}$.

Thus we get a criterion for Benford's law:

PROPOSITION 1: An infinite sequence of integers $a = \{a_n\}$ obeys Benford's law if the sequence $\{\log a_n\}_{n=1,2,\ldots}$ is uniformly distributed mod 1.

Now let us consider, in place of first digits in a_n's, first consective blocks in a_n's. That is, we denote a string of length r by $\Delta_r = (k_1,k_2,\ldots,k_r)$, $k_i = 1,2,\ldots,9$, and the number of occurrences of a_n with

$1 \le n \le N$ of which the first consecutive block of length r is identical with Δ_r by $B_N(a; \Delta_r)$. A necessary and sufficient condition for which a_n begins with Δ_r is that the following inequalities:

$$(1.6) \quad \log(k_1k_2\ldots k_r) + m \le \log a_n < \log(k_1k_2\ldots k_r+1) + m,$$

hold for some nonnegative integer m, where

$$k_1k_2\ldots k_r = k_1\cdot 10^{r-1} + k_2\cdot 10^{r-2} + \ldots + k_r.$$

DEFINITION: We say that an infinite sequence of integers $a = \{a_n\}_{n=1,2,\ldots}$ is a strong Benford sequence if, for all positive integer r and for every block Δ_r of length r,

$$(1.7) \quad \lim_{N\to\infty} \frac{B_N(a; \Delta_r)}{N} = \{\log (k_1k_2\ldots k_r+1)\} - \{\log (k_1k_2\ldots k_r)\},$$

here $\{x\}$ denotes the fractional part of x.

It is immediate that the uniform distribution mod 1 of $\{\log a_n\}$ leads to the strong Benford's sequence of $\{a_n\}$. Since the sequence $\{\log(k_1k_2\ldots k_r)\}$ for all positive integers r and for every block Δ_r of length r is dense in the unit interval $I_0 = [0,1)$, we conclude

that the converse is also true.

THEOREM 1: (P. DIACONIS [3]) *An infinite sequence of integers* $a = \{a_n\}_{n=1,2,\ldots}$ *is a strong Benford sequence if and only if* $\{\log a_n\}_{n=1,2,\ldots}$ *is uniformly distributed* mod 1.

COROLLARY: *A sequence of powers of positive integer* s *is a strong Benford sequence, unless* s *is a power of* 10.

2. BENFORD'S LAW FOR LINEAR RECURRENCE SEQUENCES

In this Section, we prove a sufficient condition for which a recurrence integer sequence of arbitrary order obeys Benford's law. We apply Proposition 1 as a criterion for Benford's law, and so linear recurrence sequences that we prove to obey Benford's law are automatically strong Benford sequences from Theorem 1.

For the sake of simplicity, we first restrict ourselves to linear recurrence integer sequences of order 2.

Consider a linear recurrence sequence $\{u_n\}_{n=1,2,\ldots}$ and we may suppose that every term u_n is a positive integer. This linear recurrence integer sequence $u = \{u_n\}$ satisfies a linear recurrence formula:

(2.1) $$u_{n+2} = a \cdot u_{n+1} + b \cdot u_n,$$

where a and b are integers.

We write the characteristic equation of (2.1) as:

(2.2) $$\lambda^2 = a \cdot \lambda + b,$$

and denote its roots by λ_1 and λ_2. We distinguish three cases according as the characteristic equation (2.2) has two distinct real roots, or double real root or complex conjugate roots.

The first two cases have already been settled completely in our earlier works [17] and [18]. Those cases can be obtained by using known results and the methods of their proofs, such as, R.L. Duncan [4], Lawerence Kuipers [12], [13] and Kuipers and Shiue [15]. Hence we discuss only the third case.

Case III: Complex conjugate roots

In this case, the roots λ_1 and λ_2 of the equation (2.2) are written by:

(2.3) $$\lambda_1 = r \cdot e^{2\pi i\theta} \quad \text{and} \quad \lambda_2 = r \cdot e^{-2\pi i\theta},$$

where r is a positive real number and θ is also real.

Now we need to divide this case III into two cases;

III-i. θ is rational in (2.3).

In this case, we put $\theta = p/q$ and we may assume without loss of generality that p and q are coprime positive integers. Then the n-th term u_n is written by

$$u_n = A\cdot(r\cdot e^{2\pi i\theta})^n + B\cdot(r\cdot e^{-2\pi i\theta})^n$$

$$= A\cdot r^n\cdot e^{2\pi i\frac{q}{p}n} + B\cdot r^n e^{-2\pi i\frac{q}{p}n}$$

$$= r^n\cdot\{A\cdot e^{2\pi i\frac{q}{p}n} + B\cdot e^{-2\pi i\frac{q}{p}n}\}.$$

Now consider the sequence $\{A_n\}$ in (2.4) defined by:

$$(2.5) \qquad A_n = A\cdot e^{2\pi i\frac{q}{p}n} + B\cdot e^{-2\pi i\frac{q}{p}n}.$$

This sequence $\{A_n\}$ is purely periodic of period p, then we divide the original recurrence integer sequence $\{u_n\}$ into p subsequence $\{u_{pn+j}\}_{n=0,1,\ldots}$, for $j = 1,2,\ldots,p$.

We now assume that

$$\log r = \log|\lambda_1| = \log|\lambda_2|$$

is irrational. Then the sequence $\{c\cdot n \log r\}_{n=1,2,\ldots}$ is uniformly distributed mod 1, where c is an arbitrary non zero constant.

Hence, unless the periodic sequence $\{A_n\}$ is a sequence of 0's, each subsequence $\{|u_{pn+j}|\}_{n=0,1,\ldots}$ is uniformly distributed mod 1 for $j = 1,2,\ldots,p$, from which we derive that the original sequence $\{|u_n|\}_{n=1,2,\ldots}$ is uniformly distributed mod 1. By making use of Proposition 1 as our criterion, we deduce that the sequence $\{u_n\}$ obeys Benford's law.

III-ii. Θ is irrational and the numbers $(1, \log r, \Theta)$ are Q-linearly independent.

We remark that thesecond assumption contains the irrationality of log r, and that the two dimensional sequence:

$$(2.6) \qquad (\{n\cdot\log r\}, \{n\cdot\Theta\})_{n=1,2,\ldots}$$

is uniformly distributed in the two dimensional unit cube $[0, 1) \times [0, 1)$ (Example 6.1 in [14]).

Now we rewrite the n-th term u_n by:

$$u_n = A\cdot(r\cdot e^{2\pi i\Theta})^n + B\cdot(r\cdot e^{-2\pi i\Theta})^n$$

$$= r^n\cdot\{A\cdot e^{-\pi i\cdot n\Theta} + B\cdot e^{-2\pi i\cdot n\Theta}\}.$$

Since the sequence $\{u_n\}$ in consideration is an integer (a fortiori, a real) sequence, it follows that the complex conjugate of u_n must be identical with u_n, from which we derive that B is the complex conjugate of A. Thus we obtain

$$u_n = r^n \cdot \{A \cdot e^{2\pi i \cdot n\theta} + \bar{A} \cdot e^{-2\pi i \cdot n\theta}\}$$

$$= r^n \cdot 2\mathrm{Re}(A) \cdot \cos\{2\pi n\theta\}, \tag{2.7}$$

where $\bar{z}$ is the complex conjugate of z and Re(z) denotes the real part of z.

The uniform distribution of (2.6) assures that, for any bounded Riemann integrable function g(x, y), which is periodic mod Z X Z,

$$\frac{1}{N} \sum_{n=1}^{N} g(n \cdot \log r, n \cdot \theta) \to \int_0^1 \int_0^1 g(x, y)\, dxdy, \tag{2.8}$$

as $N \to \infty$.

Let us put, for any nonzero integer h,

$$g_h(x, y) = e^{2\pi i h\{x + \log 2|\mathrm{Re}(A)| + \log|\cos(2\pi y)|\}}, \tag{2.9}$$

which is obviously bounded Riemann integrable and periodic mod $Z \times Z$. Substituting this function $g_h(x, y)$ into (2.8), we have

$$(2.10) \qquad \frac{1}{n} \sum_{n=1}^{N} g_h(n \cdot \log r,\ n \cdot \theta)$$

$$= \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h \cdot \log u_n} \to \int_0^1 \int_0^1 g_h(x, y)\, dxdy,$$

as $N \to \infty$.

From the theorem of Fubini, the far right side of (2.10) is shown to be zero as follows:

$$\int_0^1 \int_0^1 g_h(x, y)\, dxdy$$

$$= \int_0^1 \int_0^1 e^{2\pi i h \{x + \log 2|\mathrm{Re}(A)| + \log|\cos(2\pi y)|\}} dxdy$$

$$= e^{2\pi i \cdot \log 2|\mathrm{Re}(A)|} \int_0^1 e^{2\pi i h x}\, dx \int_0^1 e^{2\pi i h \cdot \log|\cos(2\pi y)|}\, dy$$

$$= 0.$$

Then the Weyl's criterion for uniform distribution mod 1 shows that the sequence $\{\log|u_n|\}$ is uniformly distributed mod 1, that is, $\{u_n\}_{n=1,2,\ldots}$ is a strong Benford sequence.

Now we summarize these three cases and obtain:

THEOREM 2: *Let* $\{u_n\}_{n=1,2,\ldots}$ *be an infinite sequence of positive integers which satisfies a linear recurrence formula* (2.1). *Let* λ_1 *be the root of maximum modulus of the corresponding characteristic equation* (2.2). *Then the*

sequence $\{u_n\}$ *is a strong Benford sequence if* $\log|\lambda_1|$ *is irrational and satisfies some additional technical conditions below:*

(i) *If* $a^2 + 4b > 0$, *then the constants* A *in*

$$u_n = A\lambda_1^n + B\lambda_2^n \tag{2.11}$$

is a nonzero constant, with $|\lambda_1| > |\lambda_2|$, *and if*

$$\lambda_1 = -\lambda_2 > 0, \text{ i.e. } |\lambda_1| = |\lambda_2|, \tag{2.12}$$

then either A-B *in* (2.13) *or* A+B *in* (2.14) *does not vanish, where*

$$u_{2n} = (A - B)\cdot\lambda_1^{2n} \tag{2.13}$$

and

$$u_{2n+1} = (A + B)\cdot\lambda_1^{2n+1}. \tag{2.14}$$

(ii) *If* $a^2 + 4b = 0$, *then* Cn+D *in* (2.15) *is not identically zero, where*

$$u_n = (Cn + D)\cdot\lambda_1^n. \tag{2.15}$$

(iii) *If* $a^2 + 4b < 0$, *then either* θ *in* (2.3) *is rational with infinitely many non-vanishing* A_n's *in* (2.5)

or the numbers $(1, |\lambda_1|, \Theta)$ *are* $\mathbb{Q}$*-linearly independent with irrational* Θ *and with nonzero* $\mathrm{Re}(A)$.

REMARK 2.1: The condition of the irrationality of $\log|\lambda_1|$ can be replaced by:

(2.16) λ_1 is not of the form $\pm 10^m$ for some nonnegative integer m for the cases (i) and (ii), if the coefficient a of λ in (2.2) and also in (2.1) is not zero.

Suppose that $\log|\lambda_1|$ is rational, say p/q, where p is an integer and q is a positive integer coprime to p. Then,

$$10^{\frac{q}{p}} = |\lambda_1|, \quad \text{that is,}$$

$$10^p = |\lambda_1|^q. \tag{2.17}$$

Since λ_1 is a root of the quadratic equation (2.2), the right hand side of (2.17) can be written by $c_1 \cdot |\lambda_1| + c_0$, with rational $c_0, c_1 \neq 0$, since $a \neq 0$ in the equation (2.2). Then we have

$$10^p - c_0 = c_1 \cdot |\lambda_1|. \tag{2.18}$$

$|\lambda_1|$ divides the right hand side of (2.18), then it divides also the left hand side of (2.18). Hence λ_1 must be rational.

Put $\lambda_1 = \frac{r}{s}$, where r is an integer and s is a positive integer prime to r. Substituting this λ_1 into (2.17), we have:

(2.19) $\lambda_1 = \pm 10^m$, for some nonnegative integer m, if $\log|\lambda_1|$ is rational for the real root λ_1 of (2.2) with nonzero a.

REMARK 2.2: For the case III, P. Schatte [19] independently obtained the same results.

Secondly we consider a linear recurrence sequence of positive integers $\{u_n\}_{n=1,2,\ldots}$, which satisfies the following linear recurrence formula of degree $d \geq 2$:

$$u_{n+d} = a_{d-1} \cdot u_{n+d-1} + a_{d-2} \cdot u_{n+d-2} + \ldots + a_0 \cdot u_n, \tag{2.20}$$

and also the initial conditions:

$$u_1 = c_1, \quad u_2 = c_2, \ldots, u_d = c_d, \tag{2.21}$$

and

$$\underline{a} = (a_{d-1}, a_{d-2}, \ldots, a_0) \tag{2.22}$$

and

$$\underline{c} = (c_1, c_2, \ldots, c_d)$$

are d-dimensional integral vectors.

The characteristic equation of (2.20) is

$$(2.23)\quad \lambda^d = a_{d-1}\cdot\lambda^{d-1} + a_{d-2}\cdot\lambda^{d-2} + \ldots + a_1\cdot\lambda + a_0 .$$

Throughout this Section, we assume that:

(2.24) the equation (2.23) has distinct roots $\lambda_1,\lambda_2,\ldots,\lambda_\ell$ with multiplicity $m_1,m_2,\ldots,m_\ell$, respectively and ordered according to their moduli as:

$$(2.25)\quad |\lambda_1| \geq |\lambda_2| \geq \ldots \geq |\lambda_\ell| .$$

Then the n-th term u_n can be represented by

$$(2.26)\quad u_n = b_1(n)\cdot\lambda_1^n + b_2(n)\cdot\lambda_2^n + \ldots + b_\ell(n)\cdot\lambda_\ell^n ,$$

where $b_1,b_2,\ldots,b_\ell$ are polynomials of degree at most $m_1 - 1$, $m_2 - 1,\ldots,m_\ell - 1$, respectively, that depend on $\underline{a}$, $\underline{c}$, and the roots of (2.23). We fix this representation (2.26) of u_n. (cf., e.g., Narkiewicz [22], Lemma 3.1)

We distinguish several cases according to the inequalities (2.25) and treat only the following case, since other cases have already been solved in our previous works [17], [18].

Assume that λ_1 and λ_2 are not real and are complex conjugate each other satisfying

(2.27) $$|\lambda_1| = |\lambda_2| > |\lambda_3| \geq \ldots \geq |\lambda_\ell|.$$

Assume further that

$$v_n = b_1(n)\cdot\lambda_1^n + b_2(n)\cdot\lambda_2^n$$

does not vanish for infinitely many n. Since u_n is real and

(2.28) $$u_n = v_n + o(v_n),$$

we must have

(2.29) $$b_1(n) = \overline{b_2(n)}.$$

The roots λ_1 and λ_2 are written in the form (2.3). As in the previous case of a linear recurrence sequence of order 2, we again divide this case into two cases.

i. Θ is rational.

Put $\Theta = p/q$, where p and q are coprime positive integers, then the sequence $\{e^{2\pi in\cdot\Theta}\}_{n=1,2,\ldots}$ is purely periodic of period p, then we write its first p terms by $\mu_1,\mu_2,\ldots,\mu_p$. We divide the sequence $\{v_n\}_{n=1,2,\ldots}$ into p subsequences $\{v_{np+j}\}_{n=0,1,\ldots}$, for $j = 1,2,\ldots,p$.

Then from (2.29), v_{np+j} can be written by

$$(2.30)\quad v_{np+j} = b_1(n)\cdot(re^{2\pi i\theta})^{np+j} + \overline{b_1(n)}\cdot(re^{-2\pi i\theta})^{np+j}$$

$$= r^{np}\cdot r^j\{b_1(n)\cdot\mu_j + \overline{b_1(n)}\cdot\bar{\mu}_j\}$$

$$= (r^p)^n\cdot\{r^j\cdot 2\mathrm{Re}(b_1(n)\cdot\mu_j)\}.$$

We assume further that, for all $j = 1,2,\ldots,p$,

$$(2.31)\qquad \mathrm{Re}(b_1(n)\mu_j) \neq 0.$$

Then, for all sufficiently large n, the first digit of u_n is identical with that of v_n. Each subsequence $\{v_{np+j}\}_{n=0,1,\ldots}$, for $j = 1,2,\ldots,p$ is uniformly distributed mod 1, unless log r is rational, by using, for example, one of van der Corput difference theorems. Tracing the same argument as in the linear recurrence sequence of order 2, we conclude that $\{u_n\}$ is a strong Benford sequence.

REMARK 2.3: The assumption (2.31) is necessary to guarantee that the first digit of u_n is identical with that of v_n. Without this assumption, some subsequences $\{v_{np+j}\}_{n=0,1,\cdots}$ may not be written as

$$u_{np+j} = r^j\cdot(r^p)^n\cdot(v_{np+j}\cdot r^{-j-np} + o(1)).$$

ii. Θ is irrational and the numbers $(1, \log|\lambda_1|, \Theta)$ are $\mathbb{Q}$-linearly independent. We may write $b_1(n) = a \cdot n^s \cdot e^{i\phi} + o(n^s)$ with positive a, where $s \leq m_1 - 1$ is a positive integer and m_1 is the multiplicitly of the roots λ_1 and λ_2.

LEMMA 2.1: For sufficiently large n, the distribution of the first digits of u_n is identical with that of v'_n, where

$$v'_n = a \cdot n^s \cdot r^n \cdot \cos(2\pi n\Theta + \phi). \tag{2.32}$$

PROOF: Recalling (2.28) and (2.29), we get

$$\begin{aligned} u_n &= b_1(n) \cdot \lambda_1^n + b_1(n) \cdot \bar{\lambda}_1^n + o(v_n) \\ &= \{a \cdot n^s \cdot e^{i\phi} + o(n^s)\} \cdot (r \cdot e^{2\pi i\Theta})^n + \\ &+ \{a \cdot n^s \cdot e^{i\phi} + o(n^s)\} \cdot (r \cdot e^{-2\pi i\Theta})^n + \\ &= a \cdot n^s \cdot r^n \cdot \cos(2\pi n\,\Theta + \phi) + o(n^s \cdot r^n). \end{aligned} \tag{2.33}$$

Since Θ is irrational, the sequence $\{n \cdot \Theta\}_{n=1,2,\ldots}$ is uniformly distributed mod 1. Hence there exists a positive constant K such that, for every positive ε, the set $J(\varepsilon)$ of those n's which satisfy

$$|\cos\{2\pi n\,\theta + \phi\}| \leq \varepsilon$$

has an upper density bounded by $K\varepsilon$. Hence for sufficiently large n, we have, with this ε,

$$|o(n^s \cdot r^n)| \leq K \cdot \varepsilon^2 \cdot n^s \cdot r^n,$$

where $o(n^s \cdot r^n)$ is the last o-term in (2.33). Thus, we can write

$$u_n = a \cdot n^s \cdot r^n \cos\{2\pi n\theta + \phi\} \cdot (1 + t_n),$$

with $|t_n| \leq \varepsilon$ for sufficiently large n not belonging to $J(\varepsilon)$. By passing to the limit, the assetion follows.

< Q.E.D. >

It remains to show that the sequence

$\{\log|v'_n|\}_{n=1,2,\ldots}$ is uniformly distributed mod 1.

We note that, θ being irrational, there is at most one value of n for which v'_n is zero, therefore $\log|v'_n|$ is always well-defined for all sufficiently large n.

We note that, θ being irrational, there is at most one value on for which v_n' is zero, therefore $\log |v_n'|$ is always well-defined for all sufficiently large n.

LEMMA 2.2: *Suppose the numbers* $(1,\nu,\xi)$ *are* $\mathbb{Q}$*-linearly independent. Then the sequence*

$$(\{s\cdot\log n+n\nu\},\{n\xi\})_{n=1,2,\ldots}$$

is uniformly distributed in the two dimensional unit cube $[0,1)\times[0,1)$.

PROOF. For a pair of integers (p,q) not being simultaneously equal to zero and positive integers N and M, we put

$$S_{p,q}(N) = \sum_{n=1}^{N} e^{2\pi i\{p(s\cdot\log n+n\nu)+qn\xi\}}.$$

Define M_k, for $k = 0,1,\ldots,M-1$ by

$$M_k = \{n;\ \frac{k}{M} \le \{\log n\} < \frac{k+1}{M}\}.$$

Then

$$S_{p,q}(N) = \sum_{k=0}^{M-1} \sum_{\substack{n=1 \\ n\in M_k}}^{N} e^{2i\pi\{p(s\cdot\log n+n\nu)+qn\xi\}}.$$

On the other hand,

$$\Big| \sum_{\substack{n=1 \\ n\in M_k}}^{N} e^{2\pi i\{p(s\cdot\log n+n\nu)+qn\xi\}} - e^{2\pi ips\cdot\log\frac{k}{M}} \sum_{\substack{n=1 \\ n\in M_k}}^{N} e^{2\pi i(pn\nu+qn\xi)} \Big| \leq \frac{T_k}{M},$$

where

$$T_k = \sum_{\substack{n=1 \\ n\in M_k}}^{N} 1.$$

From the uniform distribution of the sequence $(\{n\nu\},\{n\xi\})_{n=1,2,\ldots}$, we derive that

$$\sum_{\substack{n=1 \\ n\in M_k}}^{N} e^{2\pi i(pn\nu+qn\xi)} = o(T_k).$$

It is clear that

$$N = \sum_{k=0}^{M-1} T_k.$$

Henceforth, we can calculate the following estimation from above:

$$\left|\frac{1}{N}S_{p,q}(N)\right| \le \frac{1}{N}\sum_{k=0}^{M-1}\frac{T_k}{M} + \frac{1}{N}\sum_{k=1}^{N} o(T_k)$$

$$\le \frac{1}{M} + o(1), \quad \text{as} \quad N \to \infty.$$

M being arbitrary, we get

$$\lim_{N\to\infty} \frac{1}{N} S_{p,q}(N) = 0,$$

which, from the Weyl's criterion for uniform distribution, completes the proof of Lemma 2.2.

< Q.E.D. >

Now, in place of g_h in the argument (2.9), we put a bounded Riemann integrable function $G_h(x,y)$ periodic mod $Z \times Z$ defined by

$$G_h(x,y) = e^{2\pi ih\{\log a+x+\log|\cos(2\pi y+\phi)|\}},$$

for a nonzero integer h. Repeating the same argument after (2.9) in consideration with Lemma 2.2, we conclude that the linear recurrence sequence $\{u_n\}_{n=1,2,\ldots}$ is a strong Benford sequence.

REMARK 2.4: The proof of the case ii for a linear recurrence integer sequence of arbitrary order $d \geq 2$ was inspired by the discussion with G. Rauzy while his visit at Kyushu University and completed based upon our personal communications with him, to which we express our hearty thanks.

REMARK 2.5: For a real number ω, we expand it into simple continued fractions as

$$\omega = < [\omega]; a_1, a_2, \ldots, a_n, \omega_n > \tag{2.34}$$

and

$$\frac{p_n(\omega)}{q_n(\omega)} = < [\omega]; a_1, a_2, \ldots, a_n, 0 >$$

is called the n-th convergent of ω. This notion is the same as that in [8]. Then it is known that two sequences $\{p_n(\omega)\}$ and $\{q_n(\omega)\}$ satisfy a recurrence relation.

Especially for any quadratic irrational θ, the sequence $\{a_n(\theta)\}_{n=1,2,\ldots}$ of the n-th coordinate of simple continued fraction of θ is ultimately periodic from Lagrange's theorem. Henceforth the sequences $\{p_n(\theta)\}$ and $\{q_n(\theta)\}$ are unions of finitely many binary recurrence sequences.

Applying Theorem 2.1 to each binary recurrence sequence consisting of $\{p_n(\theta)\}$ and $\{q_n(\theta)\}$ with the same

argument as in the case III-i, we conclude that two sequences $\{p_n(\theta)\}$ and $\{q_n(\theta)\}$ for every real quadratic irrational θ, satisfy Benford's law.

Jager and Liardet [7] proved this result through their ingenious manipulations on $\{p_n(\theta)\}$ and $\{q_n(\theta)\}$ refining one result of Peter Kiss [10], which is different from our proof. Our proof is based on Schatte's remark [19].

Peter Schatte and Nagasaka [23] give another proof based on Schatte's idea [24].

3. BENFORD'S LAW AND SLOWLY INCREASING INTEGER SEQUENCES

In previous Sections, we have been considering rapidly increasing sequences of positive integers. In this Section, we are going to consider slowly increasing integer sequences, such as, $\{n\}_{n=1,2,\ldots}$, $\{a\cdot n^d\}_{n=1,2,\ldots}$ or the sequence of primes $\{p_n\}_{n=1,2,\ldots}$, where p_n is the n-th prime number. For these sequences, the limit of (0.1) does not exist, that is, in the sense of natural density; the sequence $\{n\}_{n=1,2,\ldots}$, for example, does not obey Benford's law.

R.L. Duncan [5] showed that the sequence $\{n\}_{n=1,2,\ldots}$ obeys Benford's law in the sense of

logarithmic density. B.J. Flehinger [6] further demonstrated that $\{n\}_{n=1,2,\ldots}$ obeys Benford's law in the sense of Banach limit.

Let us consider a polynomial sequence $\{p(n)\}_{n=1,2,\ldots}$ where $p(n)$ is a polynomial of degree at least one with integral coefficients that takes values in positive integers. In [17], we proved the following:

THEOREM 3: *Every polynomial integer sequence* $\{p(n)\}_{n=1,2,\ldots}$ *obeys Benford's law in the sense of Banach limit.*

The sequence of primes $\{p_n\}$ has been considered by several authors from the point of the distribution of first digits.

Let us denote by D_k the set of primes whose initial digits are k, for $k = 1,2,\ldots,9$. Then the Murata's (0,1)-density of D_k for the sequence of primes is defined by

$$(3.1) \qquad d_{0,1}(D_k) = \lim_{x\to\infty}\Big\{ \sum_{p\in D_k,\ p\le x} \frac{\ln p}{p} \Big/ \sum_{p\le x} \frac{\ln p}{p}\Big\},$$

if the limit exists, where p runs through the set of all primes and ln x denotes the natural logarithm of x. It is shown that this Murata's (0,1)-density is weaker than the Dirichlet density in [16]. In [8] we have proved:

THEOREM 4: *The sequence of primes* $\{p_n\}_{n=1,2,\ldots}$ *obeys Benford's law in the sense of* (0,1)*-density, that is,*

$$d_{0,1}(D_k) = \log(1 + \frac{1}{k}), \quad \textit{for} \quad k = 1,2,\ldots,9.$$

PROOF: From the prime number theorem, we can sharpen the Mertens asymptotic formula into

$$\sum_{p \le x} \frac{\ln p}{p} = \ln x + E + o(1), \tag{3.2}$$

where E is a constant. By making use of (3.2), we show that, for some positive integer m,

$$\sum_{p \in D_k, p \le (k+1)\cdot 10^m} \frac{\ln p}{p} = (m+1)\ \log(1+\frac{1}{k}) + o(m). \tag{3.3}$$

With the aid of (3.3), we can calculate the lower and upper densities of $d_{0,1}(D_k)$:

$$\underline{d_{0,1}(D_k)} \ge \lim_{n\to\infty} \{ \sum_{p \in D_k, p \le k\cdot 10^m} \frac{\ln p}{p} / \ln(k\cdot 10^n) \}$$

$$\ge \lim_{n\to\infty} \{ \sum_{p \in D_k, p \le (1+1)\cdot 10^{n-1}} \frac{\ln p}{p} / \ln(k\cdot 10^n) \}$$

$$= \lim_{n\to\infty} \frac{n\cdot\ln(1+\frac{1}{n}) + o(n)}{n\cdot\ln 10 + \ln k} = \log(1 + \frac{1}{k}).$$

Quite similarly, we get:

$$\overline{d_{0,1}(D_k)} \leq \lim_{n\to\infty}\{ \sum_{p\in D_k, p\leq (k+1)\cdot 10^m} \frac{\ln p}{p} / \ln (k\cdot 10^n)\}$$

$$= \log (1 + \frac{1}{k}).$$

<Q.E.D.>

This is however, a consequence of E. Bombieri's remark in [20] that $\{p_n\}$ obeyes Benford's law in the sense of Dirichlet (Zeta) density if we take into account the inclusion property of Riesz sums (Lemma 7.1 of Chap. 1 in [14]) pointed to us by Schatte.

REMARK 3.1: Proposition 1 is a powerful tool for Benford's law but we do not know any natural example of sequences $\{a_n\}_{n=1,2,\ldots}$ obeying Benford's law for which the sequence $\{\log a_n\}_{n=1,2,\ldots}$ is not uniformly distributed mod 1.

REMARK 3.2: For a general recurrence integer sequence $\{u_n\}_{n=1,2,\ldots}$ of arbitrary order $d > 2$, the assumption (2.25) may not be satisfied. If there exist more than three roots of maximum modulus of the corresponding characteristic equation (2.23), we do not know any satisfactory criterion for Benford's law for $\{u_n\}$.

REMARK 3.3: It might be interesting to check whether Remark 2.5 holds or not for almost all real θ in the sense of Lebesgue measure.

REMARK 3.4: There exist several densities proposed for the sequence of primes $\{p_n\}_{n=1,2,\cdots}$, such as, J. Knopfmacher [11], Daniel I. A. Cohen and Talbot M. Katz in [2] and in [9]. It is important to make a perspective study of these densities.

ACKNOWLEDGEMENT

We appreciate referee's comments pointing out some errors in the original version, to which we would like to express our sincere thanks. The revision has been done while the first author, K. Nagasaka was visiting Professor at the University of Nevada, Las Vegas. Our thanks extend also to the Department of Mathematical Sciences of University of Nevada, Las Vegas for their help.

REFERENCES

[1] ABRAMOWITZ, M. and STEGUN, I.A., *Handbook of Mathematical Functions with Formulas. Graphs and Mathematical Tables*. National Bureau of Standards (1964).

[2] COHEN, D.J.A. and KATZ, T.M., Prime numbers and the first digit phenomenon. *J. Number Theory*, 18 (1964), 261-268.

[3] DIACONIS, P., The distribution of leading digits and uniform distribution mod 1. *Ann. Prob.*, 5 (1977), 72-81.

[4] DUNCAN, R.L., An application of uniform distribution to the Fibonacci numbers. *Fibonacci Quart.*, 5 (1967), 137-140.

[5] DUNCAN, R.L., Note on the initial digit problem. *Fibonacci Quart.*, 7 (1969), 474-475.

[6] FLEHINGER, B.J.: On the probability that a random integer has initial digit A. *Amer. Math. Monthly*, 73 (1966), 1056-1061.

[7] JAGER, H., and LIARDET, P., Distributions arithmétiques des dénominateurs de convergents de fractions continues. *Indag. Mat., 91 (1988), 181-197.*

[8] KANEMITSU, S., NAGASAKA, K., SHIUE, J.-S., and RAUZY, G., Benford's law: The first digit problem. Proc. 5th Japan-USSR Symp. Prob. Theory., *Lecture Notes in Math., 1299*, Springer-Verlag, Heidelberg-New York-Tokyo (1988), 158-169.

[9] KATZ, T.M., and COHEN, D.I.A., The first digit property for exponential sequences is independent of the underlying distribution. *Fibonacci Quart.*, 24 (1984), 2-7.

[10] KISS, P., On second order recurrences and continued fractions. *Bull. Malaysian Math. Soc.*, (2), 5 (1982), 33-41.

[11] KNOPFMACHER, J., Initial digits in number theory. *Fibonacci Quart.*. 19 (1981), 121-126.

[12] KUIPERS, L., Remark on a paper by R.L. Duncan concerning the uniform distribution mod 1 of the sequence of logarithms of the Fibonacci numbers. *Fibonacci Quart.*, 7 (1969), 465-466, 473.

[13] KUIPERS, L., A property of the Fibanocci sequence (F_m), m = 0, 1,... . *Fibonacci Quart.*, 20 (1982), 112-113.

[14] KUIPERS, L., and NIEDERREITER, H., *Uniform Distribution of Sequences*. Interscience-Wiley, New York-London-Sydney-Toronto (1974).

[15] KUIPERS, L. and SHIUE, J-S., Remark on a paper by Duncan and Brown on the sequence of logarithms of certain recursive sequence. *Fibonacci Quart.*, 11 (1973), 292-294.

[16] MURATA, L., On certain densities of sets of primes. *Proc. Japan Acad. Sci. Ser. A*, 56 (1980), 351-353.

[17] NAGASAKA, K., On Benford's law. *Ann. Inst. Statist. Math.*, 35, Part A (1984), 337-353.

[18] NAGASAKA, K., and SHIUE, J.-S., Benford's law for linear recurrence sequences, *Tsukuba J. Math.*, 11 (1987), 341-351.

[19] SCHATTE, P., On the uniform distribution of certain sequences and Benford's law. *Math. Nachr.* 136 (1988), 271-273.

[20] SERRE, J.-P., *A Course in Arithmetic*. Springer-Verlag, New York (1973).

[21] VAN DER CORPUT, J.G., Diophantische Ungleichungen, *Acta Math.*, 56 (1931), 373-456.

[22] NAGASAKA, K., Data analysis and models. To appear in *Proc. Symp. on Data Analysis, Learning Symbolic and Numeric Knowledge*.

[23] SCHATTE, P. and NAGASAKA, K., A note on Benford's law for second order linear recurrences with periodical coefficients. Submitted to *Math. Nachr.*

[24] SCHATTE, P., On Benford's law for continued fractions. Submitted to *Math. Nachr.*

KENJI NAGASAKA

University of the air
2-11, Wakaba, Chiba-Shi
Chiba, 260, J a p a n

SHIGERU KANEMITSU

Department of Liberal Arts
Kinki University of Kyushu
Kayanomori, Iizuka
Fukuoka, 820, JAPAN

JAU-SHYONG SHIUE

Department of Mathematical Sciences
University of Nevada, Las Vegas
4505 Maryland Parkway
Las Vegas, NV 89154, U S A

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE DISTRIBUTION OF $p^{1/2}$ MODULO ONE

NAIR M. and PERELLI A.

INTRODUCTION

For each real $\beta\in(0,1]$, let $S(X,\Delta,\beta)$ be defined by

$$S(X,\Delta,\beta) = |\{p \le X : \{p^{1/2}-\beta\} < \Delta X^{-1/2}\}|,$$

where $\{x\}$ denotes the fractional part of x, Δ and X are positive reals with $X \ge 2$ and p denotes a prime. The study of this function arises from the pioneering work of I.M. Vinogradov [12] who showed that there are infinitely many primes p such that the inequality

$$\{p^{1/2}\} < p^{-\gamma}$$

holds, for any $\gamma < 0.1$. The best result to date is due to G. Harman [6] and A. Balog [1,2] who showed that one

can take γ to be any real <0.25. More precisely, the results of these authors imply that

$$S(X,\Delta,\beta) \sim \Delta X^{1/2}/\log X, \quad X \to \infty$$

provided that $\Delta \geq X^{1/4+\varepsilon}$.

Concerning upper bounds of the correct order of magnitude, it is easy to see that the Brun-Titchmarsh inequality implies that, for any $\beta \in (0,1]$,

$$S(X,\Delta,\beta) \ll_{\varepsilon} \Delta X^{1/2}/\log X$$

provided that $\Delta \geq X^{\varepsilon}$. Our aim is to extend the range of validity of this result to $\Delta \geq (\log X)^{\varepsilon}$. We achieve this for all algebraic β and for almost all β in $(0,1]$.

Our principal theorem concerns the slightly more general sum $S(X,\Delta,q,a)$ defined, for $a,q \in \mathbb{N}$, by

$$S(X,\Delta,q,a) = \sum_{n \leq \sqrt{X}} |\{p: n^2+2an/q-\Delta \leq p \leq n^2+2an/q+\Delta\}|.$$

THEOREM: *Let* $X \geq 2$, $q,a \in \mathbb{N}$, $q > a \geq 1$, $(a,q) = 1$, $\varepsilon,\delta > 0$.

Then

$$S(X,\Delta,q,a) \ll_{\varepsilon,\delta} \Delta X^{1/2}/\log X$$

uniformly for $q \le X^{1/2-\delta}$ *provided that* $\Delta \ge (\log q)^{\varepsilon}$. *The constant implicit in the* $\ll$ *notation is effectively computable.*

Three corollaries follow from this theorem.

COROLLARY 1: *Let* $X \ge 2$, $a/q \in (0,1]$, $(a,q) = 1$. *Then*

$$S(X,\Delta,a/q) \ll_{a/q} \Delta X^{1/2}/\log X$$

uniformly for $\Delta \ge 0$. *Further, if* $\varepsilon,\delta > 0$, *then*

$$S(X,\Delta,a/q) \ll_{\varepsilon,\delta} \Delta X^{1/2}/\log X$$

uniformly for $2 \le q \le X^{1/2-\delta}$ *and* $\Delta \ge (\log q)^{\varepsilon}$.

COROLLARY 2: *Let* $X \ge 2$ *and* $\varepsilon > 0$. *Then for all algebraic* β *in* $(0,1]$,

$$S(X,\Delta,\beta) \ll_{\beta,\varepsilon} \Delta X^{1/2}/\log X$$

provided that $\Delta \ge (\log X)^{\varepsilon}$.

COROLLARY 3: *Let* $X \ge 2$ *and* $\varepsilon > 0$. *Then for almost* $\beta \in (0,1]$,

$$S(X,\Delta,\beta) <<_{\beta,\varepsilon} \Delta X^{1/2}/\log X$$

provided that $\Delta \ge (\log X)^{\varepsilon}$.

It is also clear from the proofs of these corollaries that we can obtain a corresponding result for any β which is approximated by a/q with appropriately good information on q. Thus, for example, if there exist positive constants $c(\beta)$ and $\alpha(\geq 2)$ such that

$$|\beta - a/q| > c(\beta)/q^{\alpha}$$

for all $a/q \in Q$ then, for any $\varepsilon > 0$, we have

$$S(X,\Delta,\beta) \ll_{\varepsilon} \Delta X^{1/2}/\log X$$

provided that $\Delta \geq c_1(\beta)(\log X)^{\varepsilon}$, where $c_1(\beta)$ depends only on $c(\beta)$ and α. In particular, we obtain a result for π. This observation is due to C. Viola.

PROOF OF THE THEOREM

1. Preliminary steps. We shall initially prove the Theorem under the restrictions

$$q \leq c_1(\delta)X^{1/2-\delta} \quad \text{and} \quad \Delta \geq c_2(\varepsilon)(\log q)^{\varepsilon},$$

for some effectively computable constants $c_1(\delta)$ and $c_2(\varepsilon)$. These restrictions will then be removed at the end of the proof.

We begin by noting that if $\Delta \geq X^{1/2}$, an application of the Brun-Titchmarsh inequality directly implies the Theorem so that we may assume that $\Delta < X^{1/2}$.

Let $S = S(X,\Delta,z,q,a)$ be defined by

$$S(X,\Delta,z,q,a) =$$

$$= \sum_{n\leq X^{1/2}} \left|\{t: n^2 + \frac{2an}{q} - \Delta \leq t \leq n^2 + \frac{2an}{q} + \Delta, (t,P(z)) = 1\}\right|$$

where t denotes a natural number and $P(z) = \prod_{p<z} p$. We may write

$$S = \sum_{n\leq X^{1/2}} |\{d: |d| \leq q\Delta,\ f(n) + d = qt \text{ with } (t,P(z)) = 1\}|$$

where $f(n) = qn^2 + 2an$. We consider the following two cases separately.

CASE I, Assume that $2 \nmid q$. Then $(2a,q) = 1$ so that the condition $f(n) + d \equiv 0 \pmod q$ is equivalent to $n \equiv b \pmod q$, $0 \leq b = b(d,q,a) < q$, where b satisfies $2ab + d \equiv 0 \pmod q$. Writing $n = mq + b$ and $qb^2 + 2ab + d = cq$, the condition $f(n) + d = qt$ reduces to $f_d(m) = t$ where

$$f_d(m) = q^2m^2 + 2(bq+a)m + c.$$

Note that the range for m is $m \le (X^{1/2}-b)/q$ and that the discriminant of $f_d(m)$ is $\Delta_d = 4(qb+a)^2 - 4cq^2 = 4(a^2-qd)$.

CASE II. Assume that $2|q$. Then $(2a,q) = 2$ and let $q' = q/2$. The condition $f(n) + d \equiv 0 \pmod q$ can only be satisfied if d is even and in that case, it is equivalent to $n \equiv b \pmod{q'}$, $0 \le b = b(d,q,a) < q'$, where b satisfies $2ab + d \equiv 0 \pmod q$. Writing $n = mq'+b$ and $qb^2+2ab+d = cq$, we see that the condition $f(n)+d = qt$ reduces to $f_d(m) = t$ where

$$f_d(m) = (q')^2m^2 + (qb+a)m + c.$$

Here the range for m is $m \le (X^{1/2}-b)/q'$ and the discriminant of $f_d(m)$ is $\Delta_d = a^2-qd$. It is easy to see, in Case II, that if q' is odd and c is even then $2|f_d(m)$ for every m. Hence if q' is odd, then only those values of d, with $|d| \le q\Delta$, which give rise to odd c contribute to S. Referring to such d as "appropriate", we thus have the following reformulation for S. In Case I,

$$S = \sum_{|d| \le q\Delta} |\{m : m \le \frac{X^{1/2}-b}{q}, \ (f_d(m), P(z)) = 1\}| \qquad (1a)$$

and in Case II,

$$S = \sum_{\substack{|d| \le q\Delta, \ d \text{ even} \\ d \text{ appropriate if} \\ q' \text{ odd}}} |\{m : m \le \frac{X^{1/2}-b}{q'}, \ (f_d(m), P(z)) = 1\}| . \qquad (1b)$$

We now restrict z to

$$2 \le z \le \Delta. \qquad (2)$$

Applying Theorem 2.5 of Halberstam-Richert [5] for each value of n in the original expression for S and summing over n, we get

$$S \ll X^{1/2} \Delta \prod_{p<z} (1 - \frac{1}{p}). \qquad (3)$$

Let $\rho_d(p)$ be defined, in each case and corresponding $f_d(m)$, by

$$\rho_d(p) = |\{m \pmod p : f_d(m) \equiv 0 \pmod p\}|.$$

We now compute $\rho_d(p)$ in each of the two cases.

CASE I i) If $p = 2$ then $f_d(m) \equiv 0 \pmod 2$ reduces to $mq+c \equiv 0 \pmod 2$ so that $\rho_d(2) = 1$.

ii) If $p|q$ then $f_d(m) \equiv 0 \pmod p$ reduces to $2am+c \equiv 0 \pmod p$ so that $\rho_d(p) = 1$.

iii) If $p \nmid 2q$, then we complete the square to get

$$\rho_d(p) = |\{m \pmod p: (2q^2m+2(bq+a))^2+4q^2c-4(bq+a)^2 \equiv 0 \pmod p\}|$$

$$= |\{k \pmod p: k^2 \equiv \Delta_d \pmod p\}|, \quad \text{since } p \nmid 2q.$$

Hence, in this case, we obtain

$$\rho_d(p) = \left(\frac{\Delta_d}{p}\right) + 1.$$

CASE II i) An easy calculation shows that

$$q' \text{ even} \Rightarrow \rho_d(2) = 1,$$

$$q' \text{ odd} \Rightarrow \rho_d(2) = 0 \text{ for appropriate } d.$$

ii) If $p|q$ and $p \neq 2$, then $f_d(m) \equiv 0 \pmod p$ reduces to $am+c \equiv 0 \pmod p$ so that $\rho_d(p) = 1$.

iii) If $p \nmid q$, then completing the square as in Case I, we get

$$\rho_d(p) = \left(\frac{\Delta_d}{p}\right) + 1.$$

We note the values of $\rho_d(p)$ are very similar in the two cases. Hence, from now onwards, we shall restrict our attention exclusively to Case I. The proof of the Theorem for Case II is essentially analogous to that for Case I, but with the proviso that the extra conditions: d even, d appropriate if q' is odd be appended to every sum over d in the sequel, in addition to any conditions already present.

Since $\rho_d(p) < p$ for any p, we can apply Theorem 2.6 of [5], together with the remark at the bottom of p. 86, for each d in (1a) and sum over d to obtain

$$\frac{X^{1/2}}{q} \sum_{|d|\leq q\Delta} \prod_{p<z} \left(1 - \frac{\rho_d(p)}{p}\right) \ll S \ll \frac{X^{1/2}}{q} \sum_{|d|\leq q\Delta} \prod_{p<z} \left(1 - \frac{\rho_d(p)}{p}\right) \tag{4}$$

provided that

$$q \leq c_3 X^{1/2}, \quad z \geq c_4 \quad \text{and} \quad z \leq \left(c_5 \frac{X^{1/2}}{q}\right)^{\varepsilon_1} \tag{5}$$

where c_3, c_4, c_5 and ε_1 are fixed positive absolute constants. Hence (2), (3) and (5) imply that

$$\frac{X^{1/2}}{q} \sum_{|d|\leq q\Delta} \prod_{p<z} \left(1 - \frac{\rho_d(p)}{p}\right) \ll X^{1/2}\Delta \prod_{p<z} \left(1 - \frac{1}{p}\right) \tag{6}$$

provided that

$$\max(2, c_4) \le z \le \min(\Delta, (c_5 \frac{X^{1/2}}{q})^{\varepsilon_1}) \quad \text{and} \quad q \le c_3 X^{1/2}.$$

2. REDUCTION TO PRIMITIVE CHARACTERS

We have

$$\prod_{p<z} (1 - \frac{\rho_d(p)}{p}) = c_1(d,q,z) \prod_{p<z} (1 - \frac{1}{p}) \prod_{p<z} (1 - \frac{(\frac{\Delta_d}{p})}{p}), \tag{7}$$

where $c_1(d,q,z)$ is a partial product of an absolutely convergent infinite product with

$$1 \ll c_1(d,q,z) \ll 1. \tag{8}$$

Now given any d, write Δ_d in the form $\Delta_d = r^2 s$ with s square-free. Suppose that $s \neq 1$. Define

$$D = D_d = \begin{cases} 4s, & s \not\equiv 1 \pmod 4 \\ s, & s \equiv 1 \pmod 4. \end{cases}$$

Then it is well known (see e.g. Davenport [3]) that $Q(\sqrt{\Delta_d})$ $(=Q(\sqrt{s}))$ has discriminant D and that the Kronecker symbol $(\frac{D}{n})$ is a real primitive character

(mod D). Denote this character by $\chi(n) = \chi_d(n)$. We shall use the notation "$d \not\to \square$" to indicate values of d which give rise to $s \neq 1$ and "$d \to \square$" otherwise. We shall consider separately those values of d with $d \to \square$.

With χ defined as above, it is well known (recalling that Δ_d is even) that

$$\left(\frac{\Delta_d}{p}\right) = \chi(p) \quad \text{if} \quad p \nmid \Delta_d.$$

Hence from (7) we obtain that

$$\prod_{p<z}\left(1 - \frac{\rho_d(p)}{p}\right) = c(d,q,z) \prod_{p<z}\left(1 - \frac{1}{p}\right) \prod_{p<z}\left(1 - \frac{\chi(p)}{p}\right), \tag{9}$$

where

$$c(d,q,z) = c_1(d,q,z)c_2(d,q,z)$$

and

$$c_2(d,q,z) = \prod_{\substack{p<z \\ p \mid q\Delta_d}}\left(1 - \frac{\chi(p)}{p}\right)^{-1}$$

Let

$$c_i(d,q) = \lim_{z\to\infty} c_i(d,q,z), \quad i = 1,2$$

and define

$$c(d,q) = c_1(d,q)c_2(d,q),$$

where it is clear that the limits are well defined. For any $z \geq 2$, (8) implies, in particular, that

$$c_1(d,q) \ll c_1(d,q,z) \ll c_1(d,q). \tag{10}$$

We will need the following lemma for a corresponding statement regarding $c_2(d,q,z)$.

LEMMA 1: Let $\varepsilon > 0$. *If* $z \geq ((\log Q_1)^{\varepsilon}, 2)$, *where* $Q_1 = 32q^3\Delta$, *then*

$$c_2(d,q) \ll_{\varepsilon} c_2(d,q,z) \ll_{\varepsilon} c_2(d,q)$$

for every d *with* $|d| \leq q\Delta$.

PROOF: We have that

$$\prod_{\substack{p<z \\ p|q\Delta_d}} (1 - \frac{\chi(p)}{p})^{-1} = \prod_{p|q\Delta_d} (1 - \frac{\chi(p)}{p})^{-1} \prod_{\substack{p>z \\ p|q\Delta_d}} (1 - \frac{\chi(p)}{p}).$$

But

$$\prod_{\substack{p>z \\ p|q\Delta_d}} (1 - \frac{\chi(p)}{p}) \ll \exp(- \sum_{\substack{p>z \\ p|q\Delta_d}} \frac{\chi(p)}{p}) \ll \exp(\sum_{\substack{p>z \\ p|q\Delta_d}} \frac{1}{p}).$$

We have

$$\sum_{\substack{p \geq \log Q_1 \\ p|q\Delta_d}} \frac{1}{p} \ll \frac{\omega(q\Delta_d)}{\log Q_1} \ll \frac{\log Q_1}{\log\log Q_1 \log Q_1} = \frac{1}{\log\log Q_1}$$

so that

$$\sum_{\substack{p>z \\ p|q\Delta_d}} \frac{1}{p} = \sum_{\substack{z<p<\log Q_1 \\ p|q\Delta_d}} \frac{1}{p} + O\left(\frac{1}{\log\log Q_1}\right)$$

$$= O\left(\log\left(\frac{\log\log Q_1}{\log z}\right)\right) + O\left(\frac{1}{\log z}\right) + O\left(\frac{1}{\log\log Q_1}\right) \ll_\varepsilon 1.$$

Hence we see that

$$\prod_{\substack{p>z \\ p|q\Delta_d}} \left(1 - \frac{\chi(p)}{p}\right) \ll_\varepsilon 1.$$

For the bound in the opposite direction, note that

$$\prod_{\substack{p>z \\ p|q\Delta_d}} \left(1 - \frac{\chi(p)}{p}\right) \gg \prod_{\substack{p>z \\ p|q\Delta_d}} \left(1 + \frac{\chi(p)}{p}\right)^{-1}$$

and then apply the above argument to

$$\prod_{\substack{p>z \\ p|q\Delta_d}} \left(1 + \frac{\chi(p)}{p}\right).$$

This completes the proof of Lemma 1.

From (2), (4), (6), (9), (10) and lemma 1, we obtain, on noting that $\rho_d(p) \geq 0$, that

$$\sum_{\substack{|d| \leq q\Delta \\ d \neq \square}} c(d,q) \prod_{p<z} \left(1 - \frac{\chi(p)}{p}\right) \ll_\varepsilon q\Delta \tag{11}$$

provided that

$$q \leq c_3 X^{1/2} \quad \text{and} \quad c_6 \max((\log Q_1)^\varepsilon, 2) \leq z \leq \min\left(\Delta, c_7 \left(\frac{X^{1/2}}{q}\right)^{\varepsilon_1}\right). \tag{12}$$

3. THE AVERAGE OF $L(1,\chi)^{-1}$

We need to approximate the product in (11) by $L(1,\chi)^{-1}$ and to this end, we need to use some ideas of Elliott [4] but with z as small as possible.

Given any integer q, q not a perfect square, let $\chi \pmod D$ denote the real primitive character which q rise to, in the manner explained earlier (with q replacing Δ_d). We have

LEMMA 2: *Let* $\varepsilon > 0, T \geq 2$ *and* $z \geq \max((\log 4T)^\varepsilon, 2)$. *Then there are at most* $O_\varepsilon(T^{1/2})$ *integers* $q, |q| \leq T$, q *not a perfect square, for which the estimate*

$$L(1,\chi)^{-1} \ll_\varepsilon \prod_{p<z} \left(1 - \frac{\chi(p)}{p}\right)$$

fails. The implicit constants are effectively computable.

Lemma 2 follows from

LEMMA 3: *Let* $\varepsilon > 0, Q \geq 2$ *and* $z \geq \max((\log Q)^{\varepsilon}, 2)$. *Then there are at most* $0_{\varepsilon}(Q^{1/4})$ *primitive characters* χ *to moduli* $\leq Q$ *for which the estimate*

$$L(1,\chi)^{-1} \ll_{\varepsilon} \prod_{p<z} (1 - \frac{\chi(p)}{p})$$

fails. The implicit constants are effective.

PROOF OF LEMMA 2: Let $q = r^2 s$, s square-free and $r \geq 1$. We apply Lemma 3 with $Q = 4T/r^2$. Since $r \leq T^{1/2}$, it is clear that $Q \geq 4$ and that the modulus D of χ is $\leq Q$. Moreover, since $z \geq \max((\log 4T)^{\varepsilon}, 2)$, it is also clear that $z \geq \max((\log Q)^{\varepsilon}, 2)$. Hence, for each $r \leq T^{1/2}$, Lemma 3 implies that there are at most $0_{\varepsilon}((T/r^2)^{1/4})$ exceptional characters. The total number of exceptional q is hence

$$<<_{\varepsilon} T^{1/4} \sum_{r \leq T^{1/2}} r^{-1/2} <<_{\varepsilon} T^{1/2}$$

as required.

It remains to prove Lemma 3.

PROOF OF LEMMA 3: Clearly we may assume that Q is sufficiently large. We first show that if $U \geq Q^2$ then there are at most $0(Q^{1/20})$ primitive characters to moduli $\leq Q$ for which the estimate

$$\left| \sum_{U<p\leq 2U} \frac{\chi(p)}{p} \right| \leq Q^{-1/40} \tag{13}$$

fails. Let χ_j, $j = 1,\ldots,J$, run through the primitive characters with moduli $\leq Q$ for which (13) fails. We can write

$$\sum_{U<p\leq 2U} \frac{\chi(p)}{p} = \sum_{n=1}^{2U} a(n)\chi(n),$$

where

$$a(n) = \begin{cases} 0 & \text{if } n \leq U \text{ or if } n \neq \text{prime} \\ 1/n & \text{otherwise.} \end{cases}$$

Then, clearly,

$$\sum_{j=1}^{J} \left| \sum_{n=1}^{2U} a(n)\chi_j(n) \right|^2 \geq J\, Q^{-1/20}$$

and

$$\sum_{n=1}^{2U} |a(n)|^2 \leq \frac{2}{U}.$$

Then the duality principle implies (see Elliott [4], Lemma 22.4) that

$$J\, Q^{-1/20} \le (2U + J\, c_0\, Q \log Q)\, \frac{2}{U}$$

for some absolute constant c_0. Hence

$$J \le 4Q^{1/20} + J\, \frac{2c_0\, Q^{21/20} \log Q}{U} \le 4Q^{1/20} + \frac{1}{2} J$$

and our assertion follows.

We now subdivide the interval $[Q^2, \exp(c_8 \log^2 Q)]$, where c_8 is a suitable absolute constant to be chosen later, into $\ll \log^2 Q$ sub-intervals each of the form $(U_k, 2U_k]$, with $U_k = 2^{k-1}Q^2$. By our initial assertion, we have that for each such interval $(U_k, 2U_k]$, there are at most $0(Q^{1/20})$ characters for which (13) fails. Hence we deduce that, since

$$\left| \sum_{Q^2 \le p \le \exp(c_8 \log^2 Q)} \frac{\chi(p)}{p} \right| \le \sum_k \left| \sum_{U_k < p \le 2U_k} \frac{\chi(p)}{p} \right| \ll Q^{-1/50}, \tag{14}$$

there are at most $0(Q^{1/10})$ primitive characters to moduli $\le Q$ for which (14) fails. We shall utilise this observation later in the proof.

We now treat the range $(4\log Q)^{31} \le U \le Q$ and show that for each such U, there are at most $0(Q^{7/30})$ primitive characters to moduli $\le Q$ for which the estimate

$$\left| \sum_{U<p\le 2U} \frac{\chi(p)}{p} \right| \le U^{-1/48}$$

fails to hold. As before let χ_j, $j = 1,\ldots,J$, denote the exceptional characters. Define $a_m(n)$ by

$$\{ \sum_{U<p\le 2U} \frac{\chi(p)}{p} \}^m = \sum_{n=1}^{N} a_m(n)\chi(n),$$

with $N = (2U)^m$ and

$$m = \left[\frac{2 \log Q}{\log U} \right] + 1.$$

We have that

$$\frac{2 \log Q}{\log U} < m < \frac{4 \log Q}{\log U}$$

and that

$$a_m(n) = \frac{m!}{s_1!\ldots s_r!} \cdot \frac{1}{p_1^{s_1} \ldots p_r^{s_r}}$$

where $(s_1,\ldots,s_r)$ is uniquely defined, if it exists, by $n = p_1^{s_1}\ldots p_r^{s_r}$ where $s_i \geq 0$, $p_1,\ldots,p_r$ are all the primes in $(U,2U]$ and $s_1+\ldots+s_r = m$. If no such r-tuple exists then $a_m(n) = 0$. Thus

$$|a_m(n)|^2 \leq U^{-2m}\left(\frac{m!}{s_1!\ldots s_r!}\right)^2,$$

so that

$$\sum_{n=1}^{N}|a_m(n)|^2 \leq \frac{m!}{U^{2m}}\sum_{\substack{(s_1,\ldots,s_r)\\ s_1+\ldots+s_r=m\\ s_i\geq 0}}\frac{m!}{s_1!\ldots s_r!} = \frac{m!}{U^{2m}}r^m \leq \frac{m!}{U^m} < \left(\frac{m}{U}\right)^m \qquad (16)$$

By definition of the χ_j we have that

$$\sum_{j=1}^{J}\left|\sum_{n=1}^{N}a_m(n)\chi_j(n)\right|^2 \geq J\,U^{-\frac{m}{24}}. \qquad (17)$$

Hence, from (16), (17) and the same application of the duality principle as before, we get

$$JU^{-\frac{m}{24}} \leq ((2U)^m + J\,c_0\,Q\log Q)\left(\frac{m}{U}\right)^m,$$

i.e.

$$J \leq (2m\, U^{1/24})^m + J\, c_0\, Q \log Q \left(\frac{m}{U^{23/24}}\right)^m .$$

A simple calculation shows that

$$c_0\, Q \log Q \left(\frac{m}{U^{23/24}}\right)^m \leq \frac{1}{2}$$

provided that

$$U \geq (4 \log Q)^{12/5} \tag{18}$$

so that we obtain

$$J \leq 2(2m\, U^{1/24})^m .$$

Again, a simple calculation now shows that

$$J \ll Q^{7/30}$$

provided that $U \geq (4 \log Q)^{31}$ as claimed.

As done in the previous range, we may now subdivide the interval $[z, Q^2]$ into appropriate subintervals and use (14) and (15) to show that if $(4 \log Q)^{31} \leq z \leq \exp(c_8 \log^2 Q)$ then there are at most $O(Q^{1/4})$ primitive characters to moduli $\leq Q$ for which the estimate

$$\left| \sum_{z<p\le\exp(c_8\log^2 Q)} \frac{\chi(p)}{p} \right| \le z^{-1/50} + Q^{-1/50} \qquad (19)$$

fails to hold.

The range $U > \exp(c_8 \log^2 Q)$, for an appropriate c_8, is covered by using Page's theorem. From e.g. (18) of Nair-Perelli [9], we have that there is at most one primitive character with modulus $\le Q$ for which the estimate

$$L(1,\chi)^{-1} = \prod_{p<z} (1 - \frac{\chi(p)}{p}) \{1+0(\exp(-c_9\sqrt{\log z}))\} \qquad (20)$$

fails, provided that $z \ge \exp(c_8 \log^2 Q)$ and c_9 is a suitable positive constant.

We can complete the proof of Lemma 3. Write

$$L(1,\chi)^{-1} = \prod_{p<z} (1 - \frac{\chi(p)}{p}) \prod_{p\ge z} (1 - \frac{\chi(p)}{p})$$

and define $T(z,\chi)$ by

$$T(z,\chi) = \prod_{p\ge z} (1 - \frac{\chi(p)}{p}).$$

If $z \ge \exp(c_8 \log^2 Q)$, then (20) implies that $T(z,\chi) \ll 1$,

with at most one exceptional character. It is easy to see from (19), by considering $\log T(z,\chi)$, that

$$T(z,\chi) \ll 1$$

with at most $0(Q^{1/4})$ exceptional characters provided that

$$z \geq (4 \log Q)^{31}.$$

It remains to estimate $T(z,\chi)$ for z in the range

$$\max((\log Q)^{\varepsilon},2) \leq z < (4 \log Q)^{31}.$$

We have, in this case,

$$T(z,\chi) = \prod_{z<p<(4 \log Q)^{31}} (1 - \frac{\chi(p)}{p}) \prod_{p\geq(4 \log Q)^{31}} (1 - \frac{\chi(p)}{p}). \qquad (21)$$

But

$$\log\Big(\prod_{z<p<(4 \log Q)^{31}} (1 - \frac{\chi(p)}{p})\Big) \leq \sum_{z<p<(4 \log Q)^{31}} \frac{1}{p}$$

$$= \log(\frac{\log((4 \log Q)^{31})}{\log z}) + 0(\frac{1}{\log z}) \ll \frac{1}{\varepsilon}$$

provided that $(\log Q)^{\varepsilon} > 2$. From (21), we then deduce that

$$T(z,\chi) \ll_\varepsilon 1$$

with at most $0(Q^{1/4})$ exceptions. If $(\log Q)^\varepsilon < 2$, then Lemma 3 is clearly true with $0_\varepsilon(Q^{1/4})$ exceptions and this completes the proof of the lemma.

Let Q_2 be defined by

$$Q_2 = \max_{|d|\le q\Delta} |\Delta_d| \quad .$$

Clearly we have that $Q_2 \le 8q^2\Delta \le Q_1$.

We call "good" any d, $|d| \le q\Delta$, such that Δ_d is not an exception in the sense of Lemma 2 with $T = Q_2$ and

$$z = z_0 = c_6 \max((\log Q_1)^\varepsilon, 2)$$

and "bad" otherwise. Note that c_6 is the constant in eq. (12). We need to estimate

$$\Sigma_1 = \sum_{\substack{|d|\le q\Delta \\ d\ne\square \\ d \text{ bad}}} c(d,q) \prod_{p<z_0} \left(1 - \frac{\chi(p)}{p}\right)$$

and

$$\Sigma_2 = \sum_{\substack{|d|\le q\Delta \\ d\ne\square \\ d \text{ bad}}} c(d,q) L(1,\chi)^{-1}.$$

Clearly

$$\prod_{p<z_0} (1 - \frac{\chi(p)}{p}) \ll \log z_o \tag{22}$$

and from the definition of $c(d,q)$,

$$c(d,q) \ll \prod_{p|Q_1} (1 + \frac{1}{q}) \ll \log \log Q_1. \tag{23}$$

Hence from Lemma 2 with $T = Q_2$ and $z = z_0$, (22) and (23), we get that

$$\Sigma_1 \ll \log z_0 \log \log Q_1 \sum_{\substack{|d|\leq q\Delta \\ d \neq \square \\ d \text{ bad}}} 1 \ll_\varepsilon (\log \log Q_1)^2 Q_2^{1/2}.$$

Thus

$$\Sigma_1 \ll_\varepsilon q\Delta \tag{24}$$

provided that

$$\Delta \gg (\log \log Q_1)^4. \tag{25}$$

Using (23), we have that

$$\Sigma_2 \ll \log \log Q_1 \sum_{\substack{|d|\leq q\Delta \\ d \neq \square \\ d \text{ bad}}} L(1,\chi)^{-1}. \tag{26}$$

We now need the following lemma.

LEMMA 4: *We have that*

$$\sum_{\substack{|d|\le q_1\Delta \\ d \neq \square \\ d \text{ bad}}} L(1,\chi)^{-1} \ll_\varepsilon Q_2^{1/2} \log\log Q_2.$$

PROOF: Let $D = D_d$ be associated with d in the manner explained earlier and let $L \ge 2$ be a parameter to be chosen. Then

$$\sum_{\substack{|d|\le q_1\Delta \\ d \neq \square \\ d \text{ bad}}} L(1,\chi)^{-1} = \sum_{\substack{|d|\le q_1\Delta \\ d \neq \square \\ d \text{ bad, } D\le L}} L(1,\chi)^{-1} + \sum_{\substack{|d|\le q_1\Delta \\ d \neq \square \\ d \text{ bad, } D> L}} L(1,\chi)^{-1} =$$

$$= \Sigma_3 + \Sigma_4, \quad \text{say.} \tag{27}$$

We recall that Tatuzawa's theorem [11] implies that given any $\alpha > 0$,

$$L(1,\chi) > \frac{\alpha}{10D^\alpha}$$

for any real primitive character $\chi \pmod D$, with at most one exception.

We now estimate Σ_3 as follows. Choose $\alpha = 1/\log L$. Hence for any $D \leq L$ we have that

$$L(1,\chi)^{-1} \ll \log L$$

except for at most one $\bar{D}_1 \leq L$. Hence

$$\Sigma_3 \ll \log L \sum_{\substack{|d|\leq q_1\Delta \\ d \neq \square \\ d \text{ bad}}} 1 + \sum_{\substack{|d|\leq q_1\Delta \\ d \neq \square \\ d \text{ bad giving rise to } \bar{D}_1}} L(1,\chi)^{-1}. \tag{28}$$

Now, from Dirichlet's class-number formula, we obtain that

$$L(1,\chi)^{-1} \ll D^{1/2}$$

for any real primitive character $\chi \pmod D$. This is clear in the imaginary quadratic case while in the real quadratic case we need only note that if ξ is a fundamental unit, then

$$\xi \geq \frac{1+\sqrt{2}}{2}$$

by an examination of the size of solutions of Pell's equation.

We therefore deduce from Lemma 2 with $T = Q_2$ and $z = z_0$ and (28) that

$$\Sigma_3 \ll_\varepsilon Q_2^{1/2} \log L + (\bar{D}_1)^{1/2} \sum_{r \le \sqrt{\frac{4Q_2}{D_1}}} 1 \ll_\varepsilon Q_2^{1/2} \log L. \qquad (29)$$

In the estimate for Σ_4, i.e. with $D > L$, we apply Tatuzawa's theorem with $\alpha = 1/\log Q_2$ thus obtaining, by putting $\Delta_d = r^2 s$ and denoting by $\bar{D}_2$ the exceptional modulus if it exists,

$$\Sigma_4 \ll \log Q_2 \sum_{r \le \sqrt{\frac{4Q_2}{L}}} \sum_{\substack{s \le \frac{4Q_2}{r^2} \\ s \text{ bad}}} 1 + (\bar{D}_2)^{1/2} \sum_{\substack{|d| \le q\Delta \\ d \not\to \square \\ d \text{ bad giving rise to } \bar{D}_2}} 1. \qquad (30)$$

Using Lemma 3 with $Q = 4Q_2$ and $z = z_0$, it is clear that the bad s provided by the exceptions in Lemma 3 include the bad s in (30) so that

$$\Sigma_4 \ll \log Q_2 \sum_{r \le \sqrt{\frac{4Q_2}{L}}} \left(\frac{4Q_2}{r^2}\right)^{1/4} + Q^{1/2} \ll \frac{\log Q_2}{L^{1/4}} Q_2^{1/2} + Q_2^{1/2}. \qquad (31)$$

Hence choosing $L = (\log Q_2)^4$, we deduce from (27), (29) and (31) the assertion of Lemma 4.

From (24), (26) and Lemma 4, we obtain

$$\Sigma_1, \Sigma_2 \ll_\varepsilon q\Delta \qquad (32)$$

provided that (25) holds.

From (11), with $z = z_0$, (12) and (32), we get that

$$\sum_{\substack{|d|\le q\Delta \\ d \not\to \square}} c(d,q)L(1,\chi)^{-1} \ll_\varepsilon q\Delta \tag{33}$$

provided that

$$z_0 \le \min(\Delta, c_7(\frac{X^{1/2}}{q})^{\varepsilon_1}) \quad \text{and} \quad \Delta >> (\log\log Q_1)^4 \tag{34}$$

and

$$q \le c_3 X^{1/2} \tag{35}$$

hold.

4. CONCLUSION OF THE PROOF

We now choose

$$\bar{z} = \min((\frac{c_5 X^{1/2}}{q})^{\varepsilon_1}, X^{1/3}).$$

Then there exists $c_1(\delta) > 0$ such that if

$$q \le c_1(\delta) X^{1/2-\delta} \tag{36}$$

then both (35) and

$$X^{1/3} \geq \bar{z} \geq c_3(\delta)\, X^{\varepsilon_1 \delta}, \tag{37}$$

where $c_3(\delta)$ is a suitable constant, are satisfied. Hence we shall assume that (36) holds from now on.

By (5) we need to estimate

$$\frac{\sqrt{X}}{q} \sum_{|d|\leq q\Delta} \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) = \frac{\sqrt{X}}{q}\left(\sum_{\substack{|d|\leq q\Delta \\ d \neq \square}} + \sum_{\substack{|d|\leq q\Delta \\ d \to \square}} \right) \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right). \tag{38}$$

Clearly for any $d \to \square$ we have that

$$\prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) = \prod_{\substack{p<\bar{z} \\ p|q\Delta_d}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p<\bar{z} \\ p\nmid q\Delta_d}} \left(1 - \frac{2}{p}\right) \leq \prod_{p<\bar{z}} \left(1 - \frac{1}{p}\right)$$

so that

$$\frac{\sqrt{X}}{q} \sum_{\substack{|d|\leq q\Delta \\ d \to \square}} \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) \leq \frac{\sqrt{X}}{q}(q\Delta) \prod_{p<\bar{z}} \left(1 - \frac{1}{p}\right) \ll_\delta \frac{\Delta \sqrt{X}}{\log X}. \tag{39}$$

We now estimate the corresponding sum for $d \neq \square$. To this end, we need to compare

$$\sum_{\substack{|d|\leq q\Delta \\ d \neq \square}} \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) \quad \text{with} \quad \frac{1}{\log X} \sum_{\substack{|d|\leq q\Delta \\ d \neq \square}} c(d,q) L(1,\chi)^{-1}.$$

At this stage, we find it necessary to write the product involving $\rho_d(p)$ in terms of ideals in $Q(\sqrt{\Delta_d})$.

Let $N\mathfrak{A}$ denote the norm of an integral ideal $\mathfrak{A}$ in $Q(\sqrt{\Delta_d})$ and let $\mathfrak{p}$ denote, in general, a prime ideal in the same field. We have

LEMMA 5: *Let* $|d| \leq q\Delta$. *Then*

$$\prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) \asymp_\delta c(d,q) \prod_{Np<\bar{z}} \left(1 - \frac{1}{Np}\right).$$

The notation is as in [9] i.e. that $f \asymp g$ if $g \ll f \ll g$. The δ in this particular case indicates that the implicit constants may depend on δ.

PROOF: Using the decomposition of $\rho_d(p)$, we have that

$$\prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) = \prod_{\substack{p<\bar{z} \\ p|2q}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p<\bar{z} \\ p\nmid 2q}} \left(1 - \frac{\left(\frac{\Delta_d}{p}\right) + 1}{p}\right)$$

$$\asymp \prod_{\substack{2<p<\bar{z} \\ p|q\Delta_d}} \left(1 - \frac{1}{p}\right) \prod_{\substack{2<p<\bar{z} \\ p\nmid q\Delta_d}} \left(1 - \frac{\left(\frac{\Delta_d}{p}\right) + 1}{p}\right)$$

$$\asymp \prod_{\substack{2<p<\bar{z} \\ p \mid q\Delta_d}} \left(1 - \frac{1}{p}\right) \prod_{\substack{2<p<\bar{z} \\ p \nmid q\Delta_d \\ \left(\frac{D_d}{p}\right)=1}} \left(1 - \frac{1}{p}\right)^2$$

$$\asymp \prod_{\substack{2<p<\bar{z} \\ p \mid q\Delta_d}} \left(1 - \frac{1}{p}\right) \prod_{\substack{2<p<\bar{z} \\ p \nmid q\Delta_d \\ \left(\frac{D_d}{p}\right)=1}} \left(1 - \frac{1}{p}\right)^{-2} \prod_{\substack{2<p<\bar{z} \\ \left(\frac{D_d}{p}\right)=0}} \left(1 - \frac{1}{p}\right)^{-1} \cdot \Pi_2(\bar{z}) =$$

$$= \Pi_1(\bar{z})\ \Pi_2(\bar{z}), \quad \text{say,}$$

where

$$\Pi_2(\bar{z}) = \prod_{\substack{2<p<\bar{z} \\ \left(\frac{D_d}{p}\right)=1}} \left(1 - \frac{1}{p}\right)^2 \prod_{\substack{2<p<\bar{z} \\ \left(\frac{D_d}{p}\right)=0}} \left(1 - \frac{1}{p}\right) \prod_{\substack{4<p^2<\bar{z} \\ \left(\frac{D_d}{p}\right)=-1}} \left(1 - \frac{1}{p^2}\right).$$

By Theorem 90 of Hecke [7] we get that

$$\Pi_2(\bar{z}) \asymp \prod_{Np<\bar{z}} \left(1 - \frac{1}{Np}\right).$$

Further,

$$\Pi_1(\bar{z}) \asymp \prod_{\substack{2<p<\bar{z} \\ p\mid q\Delta_d \\ (\frac{D_d}{p})=-1}} (1+\frac{1}{p})^{-1} \prod_{\substack{2<p<\bar{z} \\ p\mid q\Delta_d \\ (\frac{D_d}{p})=1}} (1-\frac{1}{p})^{-1} \asymp \prod_{\substack{p<\bar{z} \\ p\mid q\Delta_d}} (1-\frac{\chi(p)}{p})^{-1} =$$

$$= c_2(d,q,\bar{z}), \quad \text{as defined just before eq. (10).}$$

Hence

$$\prod_{p<\bar{z}} (1-\frac{\rho_d(p)}{p}) \asymp c_2(d,q,\bar{z}) \prod_{N\mathfrak{p}<\bar{z}} (1-\frac{1}{N\mathfrak{p}}).$$

Since

$$\bar{z} \gg_\delta \max(2,(\log Q_1)^\delta),$$

Lemma 5 thus follows from Lemma 1 and (10).

We also need

LEMMA 6: *Let* $F_d(n)$ *denote the number of integral ideals with norm* n *in* $Q(\sqrt{\Delta_d})$. *Then*

$$\sum_{n\le t} F_d(n) = L(1,\chi)t + O(t^{1/2} D^{1/4} \log^{1/2} D), \quad t \to \infty.$$

PROOF. Lemma 6 was proved in [9] for imaginary quadratic fields but essentially the same proof also works for any quadratic field.

Let $\tilde{z} = \max(Q_2^6, \bar{z})$. By partial summation and using the estimate $L(1,\chi) \gg D^{-1/2}$, we obtain from Lemma 6,

as in [9], that

$$\sum_{n\le\tilde{z}} \frac{F_d(n)}{n} \gg L(1,\chi)\ \log \tilde{z}. \tag{40}$$

But

$$\prod_{Np<\tilde{z}} (1 - \frac{1}{Np})^{-1} \ge \sum_{N\mathfrak{A}<\tilde{z}} \frac{1}{N\mathfrak{A}} = \sum_{n<\tilde{z}} \frac{F_d(n)}{n},$$

so that (40) implies that

$$\prod_{Np<\tilde{z}} (1 - \frac{1}{Np}) \ll \frac{1}{L(1,\chi)\ \log \tilde{z}}.$$

Hence, from Lemma 5, we deduce that

$$\prod_{p<\tilde{z}} (1 - \frac{\rho_d(p)}{p}) \ll_\delta \frac{c(d,q)}{L(1,\chi)\ \log \tilde{z}}. \tag{41}$$

On the other hand, from (9) and Lemma 1, we have that

$$\prod_{p<\tilde{z}} (1 - \frac{\rho_d(p)}{p}) \asymp_\delta c(d,q) \prod_{p<\tilde{z}} (1 - \frac{1}{p}) \prod_{p<\tilde{z}} (1 - \frac{\chi(p)}{p}) \tag{42}$$

and

$$\prod_{p<\bar{z}} (1 - \frac{\rho_d(p)}{p}) \asymp_\delta c(d,q) \prod_{p<\bar{z}} (1 - \frac{1}{p}) \prod_{p<\bar{z}} (1 - \frac{\chi(p)}{p}). \tag{43}$$

Hence from (41) and (42) we get that

$$\prod_{p<\tilde{\tilde{z}}}(1 - \frac{\chi(p)}{p}) \ll_\delta L(1,\chi)^{-1}. \tag{44}$$

But

$$\prod_{p<\tilde{\tilde{z}}} (1 - \frac{\chi(p)}{p}) = \prod_{p<\bar{z}} (1 - \frac{\chi(p)}{p}) \prod_{\bar{z}\le p<\tilde{z}} (1 - \frac{\chi(p)}{p}) \tag{45}$$

and, by (37),

$$\prod_{\bar{z}\le p<\tilde{z}} (1 - \frac{\chi(p)}{p}) \ge \prod_{\bar{z}\le p<\tilde{z}} (1 - \frac{1}{p}) \gg_\delta 1. \tag{46}$$

From (44)-(46), we deduce that

$$\prod_{p<\bar{z}} (1 - \frac{\chi(p)}{p}) \ll_\delta L(1,\chi)^{-1}. \tag{47}$$

From (43) and (47), we get that, for $|d| \le q\Delta$,

$$\prod_{p<\bar{z}} (1 - \frac{\rho_d(p)}{p}) \ll_\delta \frac{1}{\log X} \frac{c(d,q)}{L(1,\chi)}$$

so that, by (33), we obtain that

$$\frac{\sqrt{X}}{q} \sum_{\substack{|d|\le q\Delta \\ d \ne \square}} \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) \ll_\delta \frac{1}{\log X} \sum_{\substack{|d|\le q\Delta \\ d \ne \square}} c(d,q) L(1,\chi)^{-1} \ll_{\delta,\varepsilon} \frac{\Delta\sqrt{X}}{\log X}, \tag{48}$$

provided that (34) holds. Now from (38), (39) and (48), we have that

$$\frac{\sqrt{X}}{q} \sum_{|d|\le q\Delta} \prod_{p<\bar{z}} \left(1 - \frac{\rho_d(p)}{p}\right) \ll_{\delta,\varepsilon} \frac{\Delta\sqrt{X}}{\log X}, \tag{49}$$

provided that both (34) and (36) hold.

Now given any $\varepsilon > 0$, there exists $c_9(\varepsilon) > 0$ such that (34) is satisfied provided that

$$\Delta \ge c_9(\varepsilon)(\log q)^{\varepsilon} \quad \text{and} \quad q \ge q_0(\varepsilon),$$

so that, by (36), (49) and (5), there exists $c_2(\varepsilon) > 0$ such that

$$S(X,\Delta,\bar{z},q,a) \ll_{\delta,\varepsilon} \frac{\Delta\sqrt{X}}{\log X} \tag{50}$$

provided that

$$q \le c_1(\delta) X^{1/2-\delta} \quad \text{and} \quad \Delta \ge c_2(\varepsilon)(\log q)^{\varepsilon}. \tag{51}$$

Finally, by (50), we have that

$$S(X,\Delta,q,a) \le S(X,\Delta,\bar{z},q,a) +$$

$$+ \sum_{n\le\sqrt{\bar{z}}} |\{p\le\bar{z}: n^2 + \frac{2an}{q} - \Delta \le p \le n^2 + \frac{2an}{q} + \Delta\}|$$

$$<<_{\varepsilon,\delta} \frac{\Delta\sqrt{\bar{z}}}{\log \bar{z}} + \Delta \sum_{n<<\bar{z}} 1 <<_{\varepsilon,\delta} \frac{\Delta\sqrt{\bar{z}}}{\log \bar{z}} + \Delta X^{1/3} \ll_{\varepsilon,\delta} \frac{\Delta\sqrt{\bar{z}}}{\log \bar{z}},$$

provided that (51) holds.

We now proceed to weaken the conditions (51) to those in the statement of the Theorem. We had noted at the very outset that the Brun-Titchmarsh theorem implies our theorem if $\Delta \ge X^{1/2}$ so that we can assume that $\Delta < X^{1/2}$. Hence if $X <<_{\varepsilon,\delta} 1$, we have that $\Delta <<_{\varepsilon,\delta} 1$ and so $S(X,\Delta,q,a) <<_{\varepsilon,\delta} 1$. Since $\Delta X^{1/2}/\log X >>_{\varepsilon} 1$, this would imply the Theorem. We may therefore assume that X is sufficiently large as a function of ε or δ.

Suppose then that (a) $q \le X^{1/2-\delta}$ and (b) $\Delta \ge (\log q)^{\varepsilon}$. X being sufficiently large implies that $q \le c_1(\delta/2)X^{1/2-\delta/2}$ and further $\Delta' = \max(\Delta, c_2(\varepsilon)\Delta)$ satisfies $\Delta' \ge \Delta$ and $\Delta' \ge c_2(\varepsilon)(\log q)^{\varepsilon}$.
Hence we have that

$$S(X,\Delta,q,a) \ll_{\varepsilon,\delta/2} \frac{\Delta' \sqrt{X}}{\log X} \ll_{\varepsilon,\delta} \frac{\Delta \sqrt{X}}{\log X}$$

as required.

PROOF OF COROLLARY 1

We have, for any $\beta \in (0,1]$,

$$S(X,\Delta,\beta) = |\{p \le X: \exists n \in \mathbb{N} \text{ s.t. } n \le p^{1/2} - \beta < n + \Delta X^{-1/2}\}|$$

$$= |\{p \le X: \exists n \in \mathbb{N} \text{ with } (n+\beta)^2 \le p < (n+\beta)^2 + 2(n+\beta)X^{-1/2}\Delta + \Delta^2 X^{-1}\}|$$

$$\le \sum_{n \le \sqrt{X}} |\{p: (n+\beta)^2 \le p < (n+\beta)^2 + 3\Delta\}|. \tag{52}$$

Let $\beta = a/q \in (0,1]$, with $(a,q) = 1$. Then (52) becomes

$$S(X,\Delta,\tfrac{a}{q}) \le \sum_{n \le \sqrt{X}} |\{p: q^2n^2 + 2aqn + a^2 \le q^2p < q^2n^2 + 2aqn + a^2 + 3q^2\Delta\}| =$$

$$= \sum_{n \le \sqrt{X}} |\{p: q^2n^2 + 2aqn + a^2 < q^2p < q^2n^2 + 2aqn + a^2 + 3q^2\Delta\}|, \tag{53}$$

since $q^2n^2 + 2aqn + a^2$ is never divisible by q^2. From (53), it is clear that

$$S(X,\Delta,\tfrac{a}{q}) = 0, \quad \text{if} \quad \Delta < \frac{1}{3q^2}. \tag{54}$$

When $q = 1$, i.e. when considering $S(X,\Delta,1)$, the required result follows from the results in [9]. Suppose, therefore, that $q \geq 2$ and apply the Theorem with $\varepsilon = \delta = 1/10$, 3Δ in place of $\Delta, X >>_{a/q} 1$ and $\Delta \geq (1/3)(\log q)^{1/10}$ to obtain

$$S(X,\Delta,\frac{a}{q}) \leq S(X,3\Delta+1,q,a) << \frac{\Delta\sqrt{X}}{\log X} . \tag{55}$$

It remains to consider the range $1/3q^2 \leq \Delta < (1/3)(\log q)^{10}$. Here, we have

$$S(X,\Delta,\frac{a}{q}) \leq S(X,3\Delta+1,q,a) \leq S(q^6X,10q^2\Delta\log q,q,a)$$

$$\ll \frac{(q^6X)^{1/2}10q^2\Delta\log q}{\log(q^6X)} <<_{a/q} \frac{\Delta X^{1/2}}{\log X} . \tag{56}$$

The first part of Corollary 1 follows from (54)-(56) and the second part follows from the Theorem on observing that

$$S(X,\Delta,\frac{a}{q}) \leq S(X,3\Delta+1,q,a).$$

PROOF OF COROLLARY 2

We need the following result: the inequality

$$|\beta - \frac{a}{q}| < \frac{1}{q^3}$$

has only a finite number of solutions a/q for almost all $\beta \in \mathbf{R}$. This is a special case of Theorem 32 of Khinchin [8]. As a consequence, we get that for almost all $\beta \in (0,1]$, there exists an ineffective constant $c_{10}(\beta) > 0$ such that for any a/q,

$$|\beta - \frac{a}{q}| > \frac{c_{10}(\beta)}{q^3} \tag{57}$$

holds. But from Dirichlet's approximation theorem, we have that for every $\beta \in (0,1]$ and every $L \geq 2$, there exists $q \leq L$ and $a < q$, $(a,q) = 1$ such that

$$|\beta - \frac{a}{q}| \leq \frac{1}{qL} . \tag{58}$$

A comparision of (57) and (58) shows that for almost all $\beta \in (0,1]$ and every $L \geq 2$ there exist a,q with $(a,q) = 1$ and $q \leq L$, and $c_{11}(\beta)$ such that

$$|\beta - \frac{a}{q}| \leq \frac{c_{11}(\beta)}{L^{3/2}} . \tag{59}$$

From (52), we have that, for $\Delta \geq 1$,

$$S(X,\Delta,\beta) \leq \sum_{n \leq \sqrt{X}} \Big| \{p: n^2 + \frac{2an}{q} + \{2n(\beta - \frac{a}{q}) + \beta^2\} \leq p \leq n^2 + \frac{2an}{q} +$$

$$+ \{2n(\beta - \frac{a}{q}) + \beta^2\} + 4\Delta\} \Big|. \qquad (60)$$

Choosing

$$L = \left[c_{12}(\beta) \frac{X^{1/3}}{\Delta^{2/3}} \right] + 1,$$

where $c_{12}(\beta)$ is a suitable positive constant, we deduce from (59) and (60) that

$$S(X,\Delta,\beta) \leq S(X,6\Delta,q,a)$$

and Corollary 2 now follows from the Theorem on noting that $q <<_\beta X^{1/3}$.

PROOF OF COROLLARY 3

The proof of Corollary 3 follows the outline of that of Corollary 3, but replacing Khinchin's theorem by Liouville's theorem which is effective.

Let $\beta \in (0,1]$ be an algebraic number and denote by

N and H the degree ang height of β. Then (see e.g. Stolarsky [10]) for every q, a with $(a,q) = 1$,

$$|\beta - \frac{a}{q}| \geq c_{13}(N,H)q^{-N}. \tag{61}$$

Then, in the same way as in the proof of Corollary 2, we have from (61) that for each $L \geq 2$ there exist a and q with $(a,q) = 1$ and $q \leq L$ such that

$$|\beta - \frac{a}{q}| \leq \frac{c_{14}(N,H)}{L^{N/N-1}},$$

for a suitable $c_{14}(N,H) > 0$. As in the proof of Corollary 2, on choosing

$$L = \left[c_{15}(N,H) \left(\frac{X^{1/2}}{\Delta}\right)^{\frac{N-1}{N}} \right] + 1,$$

we have that

$$S(X,\Delta,\beta) \leq S(X,6\Delta,q,a)$$

and Corollary 3 follows from the Theorem on noting that $q <<_{\beta} X^{(N-1)/N}$.

REFERENCES

[1] BALOG, A., On the fractional part of p^{Θ}. *Arch. Math.* 40 (1983), 434-440.

[2] BALOG, A., On the distribution of p^{Θ} mod 1. *Acta Math. Hung.* 45 (1985), 179-199.

[3] DAVENPORT, H., *Multiplicative Number Theory*, 2nd edition. Springer Verlag. 1980.

[4] ELLIOTT, P.D.T.A., *Probabilistic Number Theory II*. Springer Verlag, 1980.

[5] HALBERSTAM, H., RICHERT, H.-E., *Sieve Methods*. Academic Press. 1974.

[6] HARMAN, G., *On the distribution of* $\sqrt{p}$ *modulo one*. Mathematika 30 (1983), 104-116.

[7] HECKE, E., *Lectures on the Theory of Algebraic Numbers*. Translation from the 1923 German edition, Springer Verlag, 1981.

[8] KHINCHIN, A.Ya., *Continued Fractions*. Univ. Chicago Press 1964.

[9] NAIR, M., and PERELLI, A., *Sieve methods and class-number problems*. J. reine angew. Math. 367 (1986), 11-26.

[10] STOLARSKY, K.B., *Algebraic Numbers and Diophantine Approximation*. Dekker 1974.

[11] TATUZAWA, T., On a theorem of Siegel. *Japanese J. Math.* 21 (1951), 163-178.

[12] VINOGRADOV, I.M., *Special Variants of the Method of Trigonometric Sums.* in Selected Works, Springer Verlag 1985.

NAIR, M.

Dept. of Mathematics
University of Glasgow
Glasgow G12 8QW, Scotland (U.K.)

PERELLI, A.

Dipartimento di Matematica
Via L.B. Alberti 4
16132 Genova, I t a l y

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

EXTREMAL PROPERTIES FOR BASES IN ADDITIVE NUMBER THEORY

MELVYN B. NATHANSON

1. MINIMAL BASES

This paper will describe some new results and problems on minimal asymptotic bases.

Denote by N the set of all nonnegative integers. Let A be a set of integers, and let hA denote the set of all sums of h elements of A. If hA contains all sufficiently large integers, then A is an *asymptotic basis of order* h. The set A is *minimal* if A is an asymptotic basis of order h, but no proper subset of A is an asymptotic basis of order h. This means that for each element $a \in A$ there are infinitely many positive integers n, each of whose representations as a sum of h elements of A must include the integer a as a summand. Stöhr [13] first defined minimal asymptotic bases, and the earliest results were

obtained by Erdős, Härtter, and Nathanson [1,2,7,10].

It is important to note that not every asymptotic basis of order h contains a subset that is a minimal asymptotic basis of order h. Stöhr [13], for example, observed that for $h \geq 2$ the set

$$A = \{1\} \cup \{ih \ i = 0, 1, 2, \ldots\}$$

does not contain a minimal asymptotic basis of order h. In the case h = 2, Erdős and Nathanson [3] have constructed a set A with the property that, for any subset S of A, the set $A \backslash S$ is an asymptotic basis of order 2 if and only if S is finite. Since the infinite set A contains no maximal finite subset, it follows that A does not contain a minimal asymptotic basis of order 2.

Problem 1. Let $h \geq 3$. Construct an asymptotic basis A with the property that, for any subset S of A, the set $A \backslash S$ is an asymptotic basis of order h if and only if S is finite.

Erdős and Nathanson [4] have obtained a sufficient condition for an asymptotic basis of order 2 to contain a minimal asymptotic basis of order 2.

THEOREM 1. Let A be an asymptotic basis of order 2, and let r(n) denote the number of solutions of the equation $n = a + a'$, where $a, a' \in A$ and $a \leq a'$. If

$r(n) \geq c \cdot \log n$ for some constant $c > 1/\log(4/3)$ and all n sufficiently large, then A contains a minimal asymptotic basis of order 2.

Problem 2. Does the condition $r(n) > c.\log n$ for *some* constant $c > 0$ and all n sufficiently large imply that A contains a minimal asymptotic basis of order 2?

In the opposite direction, Erdős and Nathanson [6] have proved the following.

THEOREM 2. Let $t > 0$. There exists an asymptotic basis A of order 2 such that $r(n) > t$ for all n sufficiently large, but A does not contain a minimal asymptotic basis of order 2.

Problem 3. Extend Theorems 1 and 2 to asymptotic bases of orders $h \geq 3$.

The following question seems to be very difficult.

Problem 4. If A is an asymptotic basis of order 2 such that r(n) tends to infinity, then must A contain a minimal asymptotic basis of order 2?

Recall that the *counting function* A(x) of the set A is the number of positive elements of A not exceeding x. Define the *lower asymptotic density* $d_L(A)$ by $d_L(A) = \liminf A(x)/x$. If $\alpha = \lim A(x)/x$ exists, then α is called the *asymptotic density* of A, and denoted d(A).

2. FAT MINIMAL BASES

Minimal bases are an extremal class of additive bases. I shall consider here an extremal property of this extremal class, namely, minimal asymptotic bases that are as "fat" or as "thin" as possible. Using Kneser's addition theorem [9] for the lower asymptotic density of sumsets, Nathanson and Sárközy [12] recently proved the following.

THEOREM 3. Let $h \geq 2$, and let A be an asymptotic basis of order h. If B is a subset of A such that $d_L(B) > 1/h$, then there is a finite subset F of $A \backslash B$ such that $B \cup F$ is an asymptotic basis of order h.

They drew two consequences from this result.

THEOREM 4. Let $h \geq 2$, and let A be an asymptotic basis of order h such that $d_L(A) = (1/h) + \delta$, where $\delta > 0$. Let $0 < \tau < \delta$. Then there is a subset W of A with asymptotic density $d(W) = \tau$ such that $A \backslash W$ is an asymptotic basis of order h.

THEOREM 5. Let $h \geq 2$. If A is a minimal asymptotic basis of order h, then $d_L(A) \leq 1/h$.

Nathanson and Sárközy [12] showed that the estimate above is best possible.

THEOREM 6. For every $h \geq 2$ there exist minimal asymptotic bases A of order h with $d(A) = 1/h$.

The proof of the theorem is by the somewhat complicated construction of explicit examples. The idea is as follows: Let $A = B \cup C$, where $B = \{b_i\}$ is a set of positive integers such that $b_i \equiv 1 \pmod{h}$ for all i, and b_{i+1}/b_i tends to infinity, and where C consists of all nonnegative multiples of h. Then A is an asymptotic basis of order h with $d(A) = 1/h$. One can construct inductively a subset C' of C such that $C \backslash C'$ has density 0 and $A' = B \cup C'$ is minimal asymptotic basis of order h. Clearly, $d(A') = 1/h$.

It is worth noting that the preceding theorems are among the few concerning minimal asymptotic bases that hold for all orders $h \geq 2$, and not just $h = 2$.

Problem 5. Let $h \geq 2$. Does there exist a minimal asymptotic basis A of order h such that $A(x) = x/h + O(1)$?

Examination of the proof of Theorem 6 in the case $h = 2$ shows that it produces a minimal asymptotic basis $A = \{a_i\}$ of order 2 such that $a_{i+1} > a_i$ and $\limsup (a_{i+1} - a_i) = 4$. It is easy to show that there cannot exist a minimal asymptotic basis $A = \{a_i\}$ of order 2 with $\limsup (a_{i+1} - a_i) = 2$.

Problem 6. Does there exist a minimal asymptotic basis $A = \{a_i\}$ of order 2 with $\limsup (a_{i+1} - a_i) = 3$?

Erdős and Nathanson [5] have improved Theorem 6 in the case $h = 2$ in the following way.

THEOREM 7. For every $\alpha \in (0, 1/2]$ there exists a minimal asymptotic basis A of order 2 with asymptotic density $d(A) = \alpha$.

Problem 7. Let $h \geq 3$. Show that for every $\alpha \in (0, 1/h]$ there exists a minimal asymptotic basis A with $d(A) = \alpha$.

3. THIN MINIMAL BASES

The above results concern minimal asymptotic bases that are as "fat" as possible. I shall now consider the construction of "thin" minimal asymptotic bases.

A simple counting argument shows that an asymptotic basis A of order h must satisfy $A(x) > c \cdot x^{1/h}$ for some $c > 0$ and all x sufficiently large. An asymptotic basis A is *thin* if $A(x) < c' x^{1/h}$ for some $c' > 0$ and all x sufficiently large. Nathanson [10] constructed the first example of a thin minimal asymptotic basis of order 2. Recently, this construction was generalized to produce minimal asymptotic bases of order h for every $h \geq 2$ [11].

THEOREM 8. Let $h \geq 2$. There exists a minimal asymptotic basis A of order h such that

$$c \cdot x^{1/h} < A(x) < c' x^{1/h}$$

for positive constants c and c' and all x sufficiently large.

Jia and Nathanson [8] have improved this as follows.

THEOREM 9. Let $h \geq 2$ and let $\tau \in [1/h, 1)$. There exists a minimal asymptotic basis A of order h such that

$$c \cdot x^{\tau} < A(x) < c' x^{\tau}$$

for positive constants c and c' and all x sufficiently large.

The examples of minimal asymptotic bases in Theorems 8 and 9 are all constructed by the following method: If W is a subset of the nonnegative integers N, let A(W) consist of all numbers of the form $\Sigma_{f \in F} 2^f$, where F is a finite, nonempty subset of W. Let $N = W_0 \cup W_1 \cup \ldots \cup W_{h-1}$ be a partition of N into pairwise disjoint, nonempty sets. Then the set

$$(*) \qquad A = A(W_0) \cup A(W_1) \cup \ldots \cup A(W_{h-1})$$

is an asymptotic basis of order h. If the partition is chosen appropriately, the basis A is minimal.

Not every partition, however, gives rise to a minimal basis. In the case h = 2, Nathanson [11] gave an example of a partition $N = W_0 \cup W_1$ such that the corresponding asymptotic basis $A = A(W_0) \cup A(W_1)$ is not a minimal asymptotic basis of order 2.

Problem 8. Let $h \geq 2$. Determine the partitions of N into h sets $N = W_0 \cup W_1 \cup \ldots \cup W_{h-1}$ such that the set A defined by (*) is *not* a minimal asymptotic basis of order h.

REFERENCES

[1] P. ERDŐS, Einige Bemerkungen zur Arbeit von A. Stöhr "Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe," *J. reine angew. Math.* 197 (1957), 216-219.

[2] P. ERDŐS and E. HÄRTTER, Konstruction von nichtperiodischen Minimalbasen mit der dichte 1/2 für die Menge der nichtnegativen ganzen Zahlen, *J. reine angew. Math.* 221 (1966), 44-47.

[3] P. ERDŐS and M. B. NATHANSON, Oscillations of bases for the natural numbers, *Proc. Amer. Math. Soc.* 53 (1975), 253-258.

[4] P. ERDŐS and M. B. NATHANSON, Systems of distinct representatives and minimal bases in additive number

[4] P. ERDÖS and M.B. NATHANSON, Systems of distinct representatives and minimal bases in additive number theory, in: M. B. Nathanson, ed., *Number Theory, Carbondale 1979*, Lecture Notes in Mathematics, vol. 751, Springer-Verlag, Berlin-New York, 1979, pp. 89-107.

[5] P. ERDÖS and M. B. NATHANSON, Minimal asymptotic bases with prescribed positive densities, *Illinois J. Math.* 32 (1988).

[6] P. ERDÖS and M. B. NATHANSON, Additive bases with many representations, *Acta Arith.* 52 (1989).

[7] E. HÄRTTER, Ein Beitrag zur Theorie der Minimalbasen, *J. reine angew. Math. 196* (1956), 170-204.

[8] X.-D. JIA and M. B. NATHANSON, A simple construction of minimal asymptotic bases, *Acta Arith.* 52 (1989).

[9] M. KNESER, Abschätzungen der asymptotischen Dichte von Summenmengen, *Math. Zeit.* 58 (1953), 459-484.

[10] M. B. NATHANSON, Minimal bases and maximal nonbases in additive number theory, *J. Number Theory* 6 (1974), 324-333.

[11] M. B. NATHANSON, Minimal bases and powers of 2, *Acta Arith.* 51 (1988).

[12] M. B. NATHANSON and A. SÁRKÖZY, On the maximum density of minimal asymptotic bases, *Proc. Amer. Math. Soc.*, (to appear)

[13] A. STÖHR, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, II, *J. reine angew.* Math. 194 (1955), 111-140.

MELVYN B. NATHANSON
Provost and Vice President
for Academic Affairs Lehman College (CUNY)
Bronx, New York 10468

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON PRODUCTS OF SEQUENCES OF INTEGERS

C. POMERANCE[1] and A. SÁRKÖZY[2]

1. INTRODUCTION

In this paper our goal is to show that if **A** and **B** are "dense" sets of integers then there are "many" distinct products of the form **ab** where $a \in A$, $b \in B$. Furthermore, we will show that this fact can be applied to study certain multiplicative "hybrid problems", i.e., multiplicative problems involving both general sets and special sets.

In 1960, Paul Erdős [1] showed the following, surprising result: the number of distinct integers of

---

[1] Research supported in part by an NSF grant.

[2] Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1811.

the form ab where a, b are natural numbers not exceeding x is

$$(1.1) \qquad x^2(\log x)^{-\alpha+o(1)} ,$$

where $\alpha = 1 - \log\{e \log 2)/\log 2 = 0.0860\ldots$. Thus we have the seemingly paradoxical result that only $o(x^2)$ integers may be found in the "multiplication table" of the integers up to x.

This paradox may be explained via the function $\nu(n)$, the number of distinct prime factors of n. It has been known since Hardy and Ramanujan [3] that the normal order of $\nu(n)$ is loglog n. Thus a "normal product" of integers $a,b \le x$ would have about 2 loglog x prime factors, which is quite *abnormal* for integers below x^2. In fact, the bulk of the products ab making up the count (1.1) come from factors a, b with less than the normal number of prime factors.

Thus it should be expected that if a certain thin subset is deleted from the set of integers up to x, then in fact there should be considerably fewer products ab than the count in (1.1). Indeed this is true and easy to see using the results in the aforementioned paper of Hardy and Ramanujan (see (2.14) below). By taking

$$A = B = \{n \le x : \nu(n) \ge \text{loglog } x - (\text{loglog } x)^{2/3}\},$$

then $|A| = |B| = (1 + o(1))x$, while

$$(1.2) \qquad |AB| \leq x^2 (\log x)^{1-2 \log 2 + o(1)}$$

where $|\ |$ denotes the cardinality of the enclosed set and AB denotes the set of products ab where $a \in A$, $b \in B$.

It may be asked if the drop in the exponent from $-\alpha$ to $1 - 2 \log 2$ between (1.1) and (1.2) can be induced to drop still further by choosing the sets A, B a bit thinner. The principal result in this paper is that the expression on the right of (1.2) essentially gives the correct lower bound for $|AB|$ so long as A, B are "dense". We shall prove the following result.

THEOREM 1. If $\varepsilon > 0$, $\delta > 0$ are arbitrary, then there exists some $x_0 = x_0(\varepsilon, \delta)$ such that if $x > x_0$, $A, B \subset \{1, 2, \ldots, [x]\}$ and

$$(1.3) \qquad |A| > \varepsilon x, \quad |B| > \varepsilon x,$$

then

$$(1.4) \qquad |AB| > x^2 (\log x)^{1-2 \log 2 - \delta}$$

Section 2 below will be devoted to proving Theorem 1. It should be noted that the method of proof could

also be used to treat the case when the ε in the theorem is not fixed, but allowed to tend to 0 "slowly". In section 3 it will be shown that the numerousness of the product set **AB** given by (1.4) implies there are products that are "close" to some number of a special sequence. Specifically, the special sequences considered are the primes and the integers free of large prime factors.

Fianally we remark that Theorem 1 implies we have equality in (1.2)

2. PROOF OF THEOREM 1

We begin by showing that we may replace **A** by a "dense" subset A_0 such that the elements of A_0 do not have too many prime factors, all have the same largest square factor and are all in an interval of the form $[u,2u]$ (and similarly for the set **B**).

Let $t(n)$ denote the largest integer such that $t(n)^2 | n$. If t is a natural number, then the number of $n \leq x$ with $t(n) > t$ is at most

$$\sum_{i=t+1}^{\infty} \left[\frac{x}{i^2}\right] < x \sum_{i=t+1}^{\infty} \frac{1}{i^2} < x \int_t^{\infty} \frac{1}{s^2}\, ds = \frac{x}{t} \quad .$$

Thus if A' is the set of $a \in A$ with $t(a) \leq 1 + 2/\varepsilon$, then

$$|A'| > \frac{\varepsilon}{2} x \ .$$

Hence, if $A(t)$ is the set of $a \in A$ with $t(a) = t$, then there is some

$$t_0 \leq 1 + 2/\varepsilon$$

with

$$|A(t_0)| > \frac{\varepsilon}{2(1+2/\varepsilon)} x > \frac{\varepsilon^2}{6} x \ .$$

Let R be an integer so that

$$2^{-R} \leq \frac{\varepsilon^2}{12} < 2^{-R+1} \ ,$$

i.e., $R = [\log_2(12/\varepsilon^2)]$. Then

$$\frac{\varepsilon^2}{6} x < |A(t_0)| \leq 2^{-R}x + \sum_{r=1}^{R} |A(t_0) \cap [2^{-r}x, \ 2^{-r+1}x]|$$

$$\leq \frac{\varepsilon^2}{12} x + R \cdot \max_{1 \leq r \leq R} |A(t_0) \cap [2^{-r}x, \ 2^{-r+1}x]|$$

implies there is some u of the form $2^{-r}x$ with

$$|A(t_0) \cap [u, 2u]| > \frac{\varepsilon^2}{12R} x \ .$$

Let A_0 be the set of $a \in A(t_0) \cap [u,2u]$ with

(2.1) $\quad \nu(a) \le [\text{loglog } x + (\text{loglog } x)^{2/3}] := T$.

Since by [3] the number of $a \le x$ for which (2.1) fails is $o(x)$, we have, for large x,

(2.2) $\quad |A_0| > \frac{\varepsilon^2}{13R} x$.

To summarize, A_0 is a subset of A for which (2.2) holds and every member a of A_0 satisfies $t(a) = t_0$, $u \le a \le 2u$ and (2.1). Similarly there are numbers t_1, v such that if B_0 is the set of $b \in B$ for which $t(b) = t_1$, $v \le b \le 2v$ and $\nu(b)$ satisfies (2.1), then $|B_0| > (\varepsilon^2/(13R))x$.

Let D denote the set of integers $d = a/t_0^2$ where $a = A_0$ and similarly let E denote the set of integers $e = b/t_1^2$ where $b \in B_0$. Then every member of A_0B_0 is of the form $dt_0^2t_1^2$ where $d \in D$, $e \in E$, so that

(2.3) $\quad |AB| \ge |A_0 B_0| = |DE|$.

Thus is suffices to estimate $|DE|$.

Note that

(2.4) $\quad |D|, |E| > \frac{\varepsilon^2}{13R} x$,

every member of $\mathbf{D}$, $\mathbf{E}$ is squarefree with at most T distinct prime factors and

$$(2.5) \qquad \mathbf{D} \subset \left[\frac{u}{t_0^2}, \frac{2u}{t_0^2}\right], \quad \mathbf{E} \subset \left[\frac{v}{t_1^2}, \frac{2v}{t_1^2}\right]$$

where $2u, 2v \le x$.

Let us denote the number of solutions of

$$de = n, \quad d \in \mathbf{D}, \quad e \in \mathbf{E}$$

by $f(n)$. By the Cauchy-Schwarz inequality we have

$$(2.6) \qquad |\mathbf{DE}| = \sum_{f(n)>0} 1 \ge \left(\sum_n f(n)\right)^2 / \sum_n f(n))^2 .$$

In view of (2.4) we have

$$(2.7) \qquad \sum_n f(n) = |\mathbf{D} \times \mathbf{E}| = |\mathbf{D}||\mathbf{E}| > \frac{\varepsilon^4}{169R^2} x^2 ,$$

so that it suffices to give an upper bound for the mean square

$$M_2 := \sum_n (f(n))^2 = \sum_n \Big(\sum_{\substack{de=n \\ d\in\mathbf{D}, e\in\mathbf{E}}} 1 \Big)^2 = \sum_{\substack{d_1e_1=d_2e_2 \\ d_1,d_2\in\mathbf{D} \\ e_1,e_2\in\mathbf{E}}} 1 .$$

In other words, M_2 denotes the number of solutions of

$$d_1e_1 = d_2e_2,\ d_1,\ d_2 \in \mathbf{D} \text{ and } e_1,\ e_2 \in \mathbf{E}$$

or, in equivalent form,

$$\frac{d_1}{d_2} = \frac{e_2}{e_1},\ d_1,\ d_2 \in \mathbf{D} \text{ and } e_1,\ e_2 \in \mathbf{E} .$$

Let us write the rational number in this equation in reduced form:

$$(2.8) \qquad \frac{d_1}{d_2} = \frac{e_2}{e_1} = \frac{p}{q}, \text{ where } (p,q) = 1 .$$

It follows from (2.5) that $1/2 \le p/q \le 2$ and thus there is a positive integer $k \le [1 + \log x]$ with

$$(2.9) \qquad e^{k-2} < p,q \le e^k .$$

By (2.8) there exist positive integers r, s such that

$$(2.10) \qquad d_1 = rp,\ d_2 = rq,\ e_2 = sp,\ e_1 = sq .$$

By (2.9) we have

$$(2.11) \qquad r = \frac{d_1}{p} \le \frac{x}{e^{k-2}},\ s = \frac{e_2}{p} \le \frac{x}{e^{k-2}} .$$

By (2.10) and the fact that $d_1, d_2 \in D$, $e_1, e_2 \in E$ we have

$$\nu(d_1) = \nu(r) + \nu(p) \le T, \ \nu(d_2) = \nu(r) + \nu(q) \le T,$$

$$\nu(e_2) = \nu(s) + \nu(p) \le T, \ \nu(e_1) = \nu(s) + \nu(q) \le T$$

and hence

$$(2.12) \quad \max(\nu(r), \nu(s)) + \max(\nu(p), \nu(q)) \le T .$$

From (2.9), (2.11) and (2.12) there exist integers $1 \le k \le [1 + \log x]$ and $0 \le \ell \le T$ with

$$p,q \in \{n \le e^k : \nu(n) \le \ell\} ,$$

$$r,s \in \{n \le x/e^{k-2} : \nu(n) \le T - \ell\} .$$

Hence the number M_2 of quadruplets p, q, r, s is not greater than

$$M_2 \le \sum_{k=1}^{[1+\log x]} \sum_{\ell=0}^{T} |\{n \le e^k : \nu(n) \le \ell\}|^2 \, |\{n \le e^{k-2} : \nu(n) \le T - \ell\}|^2$$

$$(2.13) \quad \le T^3 \sum_{k=1}^{[1+\log x]} \max_{i+j \le T} (\pi_i(e^k) \, \pi_j(\frac{x}{e^{k-2}}))^2 ,$$

where by $\pi_t(y)$ we mean the number of $n \le y$ with $\nu(n) = t$.

From [3] we have absolute positive constants c_1, c_2 such that for all natural numbers t and every $y \geq 3$

$$\pi_t(y) \leq c \frac{y}{\log y} \frac{(\operatorname{loglog} y + c_2)^{i-1}}{(i-1)!} . \tag{2.14}$$

Thus for $1 \leq k \leq [1 + \log x]$ and $i + j \leq T$ we have

$$\pi_i(e^k)\ \pi_j\left(\frac{x}{e^{k-2}}\right) \ll \frac{e^k}{k} \cdot \frac{(\log k + c_2)^{i-1}}{(i-1)!} \cdot$$

$$\cdot \frac{x\, e^{-k+2}}{\log(xe^{-k+2})} \cdot \frac{(\operatorname{loglog}(xe^{-k+2}) + c_2)^{j-1}}{(j-1)!} \ll$$

$$\ll \frac{x}{k(\log x - k)} \cdot \frac{1}{(i+j-2)!} \binom{i+j-2}{i-1} (\log k + c_2)^{i-1} \tag{2.15}$$

$$(\operatorname{loglog}(x^{e^{-k+2}}) + c_2)^{j-1} \leq \frac{x}{k(\log x - k)} \cdot$$

$$\cdot \frac{1}{(i+j-2)!} (\log k + \operatorname{loglog}(xe^{-k+2}) + 2x_2)^{i+j-2} .$$

Since $\log k + \operatorname{loglog}(xe^{-k+2}) > \operatorname{loglog} x$, we have from (2.15) that

$$\pi_i(e^k)\ \pi_j\left(\frac{x}{e^{k-2}}\right) \ll \frac{x}{k(\log x - k)}$$

$$(2.16)\quad \left(\frac{T}{\log\log x}\right)^{T-(i+j-2)} \frac{(\log k + \log(\log x - k) + c_3)^T}{T!}$$

$$\ll L(x) \frac{x}{k(\log x - k)} \frac{(\log k + \log(\log x - k))^T}{T!}$$

where $L(x) := \exp\{(\log\log x)^{2/3} + (\log\log x)^{1/3}\} =$
$= (\log x)^{o(1)}$.

Since the terms $k = \ell$ and $k = \log x - \ell$ play a symmetric role in (2.16) we obtain from (2.13) that

$$M_2 \ll L(x)^3 \sum_{k=1}^{[\frac{1}{2}\log x + 1]} \left(\frac{x}{k(\log x - k)} \frac{e^T(\log k + \log(\log x - k))^T}{T^T}\right)^2$$

$$\ll \frac{x^2\, L(x)^3}{(\log x)^2} \sum_{k=1}^{[\frac{1}{2}\log x + 1]} \frac{e^{2T}}{k^2} \left(\frac{\log k + T}{T}\right)^{2T}$$

$$\le x^2\, L(x)^5 \sum_{1\le\ell\le\log[\frac{1}{2}\log x + 1]} \sum_{k=[e^{\ell-1}]}^{[e^{\ell}]} \frac{1}{k^2} \left(1 + \frac{\log k}{T}\right)^{2T}$$

$$(2.17) \quad \ll x^2 L(x)^5 \sum_{1 \le \ell \le \log[1/2 \log x + 1]} \frac{1}{e^\ell} \left(1 + \frac{\ell}{T}\right)^{2T} .$$

Writing $F(u) = e^{-u}(1 + u/T)^{2T}$ it is easy to see that the function $F(u)$ is increasing on $0 \le u \le T$. Thus from (2.17) we obtain

$$(2.18) \quad M_2 \ll x^2 L(x)^5 (\log\log x) \frac{2^{2T}}{e^T} \ll x^2 L(x)^6 \left(\frac{4}{e}\right)^{\log\log x}$$
$$= x^2 (\log x)^{2\log 2 - 1} L(x)^6 .$$

Finally, putting (2.18) into (2.6) and using (2.3) and (2.7) we have

$$(2.19) \quad |AB| \gg \frac{\varepsilon^4}{169R^2 L(x)^6} x^2 (\log x)^{1-2\log 2}$$

where the implied constant is absolute. Sinde $L(x) = (\log x)^{o(1)}$ and $R \ll \log(1/\varepsilon)$, we have our theorem.

REMARK. By changing the definition of T in (2.1) to $[(1 + \eta(x))\log\log x]$ where $\eta(x) \to 0^+$ sufficiently slowly, the above proof would give a stronger result where ε is allowed to be any function of the form $1/(\log x)^{o(1)}$. In

fact if $\delta > 0$ is fixed in the theorem, we may choose ε as small as $1/(\log x)^{c_4\delta}$ where $c_4 > 0$ is some absolute constant.

3. APPLICATIONS

In a recent paper, Iwaniec and Sárközy [6] proved that if A, B are "dense" sets of integers, then there is a product $ab \in AB$ which is "near" a square. Specifically, they showed that if $A, B \subset \{1,2,\ldots,[x]\}$, $|A|, |B| > \varepsilon x$, then for $x \geq x_1(\varepsilon)$ there is a solution to the inequality

$$|ab - n^2| < (x \log x)^{1/2}, \quad a \in A, \ b \in B, \ n \in Z \ .$$

A result such as this does not immediately follow from Theorem 1 above since the number of integers $m \leq x^2$ such that

$$|m - n^2| < (x \log x)^{1/2}$$

for some integer n is $\ll x^{3/2}(\log x)^{1/2}$.

However, there are special sets other than the squares for which an easy application of Theorem 1 gives a result that appears to be worth stating.

THEOREM 2. Let $\varepsilon > 0$, $\delta > 0$ be arbitrary. Then there exists a constant $x_0 = x_0(\varepsilon,\delta)$ such that if $x \geq x_0$, $A, B \subset \{1,2,\ldots,[x]\}$ and $|A|, |B| > \varepsilon x$, then there exist $a \in A$, $b \in B$ and a prime p such that

$$(3.1) \qquad |ab - p| < x^{1/5 + \delta} .$$

Assuming the Riemann hypothesis, the right side of (3.1) may be replaced with $(\log x)^{1+2 \log = +\delta}$

THEOREM 3. With the same hypotheses as Theorem 2 there is an $x_0 = x_0(\varepsilon,\delta)$ such that if $x \geq x_0$ then for any $y \geq \exp\{(\log x)^{5/6 + \delta}\}$ there is a solution to the inequality

$$|ab - n| \leq y \cdot \exp\{(2 \log x)^{1/6}\}, \quad a \in A, \ b \in B$$

where no prime factor of n exceeds y. Moreover if $\eta > 0$ is arbitrary, then there is an $x_1 = x_1(\varepsilon,\delta,\eta)$ such that if $x \geq x_1$, there is a solution to the inequality

$$|ab - n| \leq x^{\delta}, \quad a \in A, \ b \in B$$

where no prime factor of n exceeds x^{η}.

(Note that the full strength of Theorem 1 is needed only in the proof of the second half of Theorem 2, while

the first half of Theorem 2 and Theorem 3 follow from any estimate of the type $|\mathbf{AB}| > x^2(\log x)^{-c}$, and, in fact, this can be proved much more easily with, say, $c = 2 \log 2 + \delta$.)

PROOF OF THEOREM 2. Let p_n denote the n-th prime. A theorem of Harman [4] is that

$$(3.2) \qquad \sum_{\substack{p_n \le x \\ p_{n+1}-p_n \ge x^{\frac{1}{10}+\delta}}} (p_{n+1} - p_n) << \frac{x}{\log x}$$

for any fixed $\delta > 0$. Replacing δ by $\frac{1}{2}\delta$ and x by x^2 in this result, Theorem 1 implies there is some ab with $a \in \mathbf{A}$, $b \in \mathbf{B}$ that is not in any interval $[p_n, p_{n+1}]$ with $p_n \le x^2$ and $p_{n+1} - p_n \ge x^{\frac{1}{5}+\delta}$. Then the closest prime p to ab satisfies (3.1).

Now assume the Riemann hypothesis holds. From Selberg [7] we have

$$\sum_{\substack{p_n \le x \\ p_{n+1}-p_n \ge H}} (p_{n+1} - p_n) << \frac{x}{H} (\log x)^2$$

uniformly for all $H \ge 1$. Thus our result follows by replacing x with x^2 and choosing $H = (\log x)^{1+2 \log 2 + \delta}$.

REMARK. In [5], Harman announced a result analogous to (3.2) with 1/10 replaced by 1/12 and with x/log x replaced by o(x). If this o(x) can be improved to $x(\log x)^{1-2\log 2-\delta}$, then the 1/5 in (3.1) can be replaced with 1/6.

PROOF OF THEOREM 3. The first result follows immediately from Theorem 1 above and Theorem 6 in Friedlander and Lagarias [2] while the second result follows from Theorem 1 above and Theorem 5 in [2].

REFERENCES

[1] P. ERDŐS, An asymptotic inequality in the theory of numbers, *Vestnik Leningrad Univ.* 15 (1960), 41-49 (in Russian).

[2] J.B. FRIEDLANDER and J.C. LAGARIAS, On the distribution in short intervals of integers having no large prime factor, *J. Number Theory* 25 (1987), 249-273.

[3] G.H. HARDY and S. RAMANUJAN, The normal number of prime factors of a number n, *Quarterly J. Math.* 48 (1920), 76-92.

[4] G. HARMAN, Primes in short intervals, *Math. Z.* 180 (1982), 335-348.

[5] G. HARMAN, On the distribution of αp mod one, *J. London Math. Soc.* (2) 27 (1983), 9-18.

[6] H. IWANIEC and A. SÁRKÖZY, On a multipliative hybrid problem, *J. Number Theory* 26 (1987), 89-95.

[7] A. SELBERG, On the normal density of primes in short intervals and the difference between consecutive primes, *Arch. Math. Naturvid.* 47 (1943), 87-105.

A. SÁRKÖZY
MTA MKI
Budapest
Reáltanoda u. 13-15.
H-1053

C. POMERANCE
Department Mathematics
University of Georgia
Athens Georgia
U S A

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

THE EDGE OF A GOLDEN SEMIGROUP

PORTA H. and STOLARSKY K.B.*

1. INTRODUCTION

It is well known that if α is the golden mean (i.e. $\alpha > 1$ and $\alpha^2 = \alpha + 1$) then the set of fractional parts $\{n\alpha\}$, where $n = 1,2,3,\ldots$, is uniformly distributed in $[0,1]$. We have discovered that not only is the downscaled sequence $\{n\alpha\}/\alpha$ uniformly distributed in $[0,1/\alpha]$, but that it is also a *multiplicative semigroup*. In fact,

$$(1) \qquad (\{n\alpha\}/\alpha)\ (\{m\alpha\}/\alpha) = \{(m*n)\alpha\}/\alpha$$

where

$$(2) \qquad m * n = mn + [\alpha m][\alpha n].$$

Proofs and generalizations of this result shall appear elsewhere. Here we shall relate the distribution of $\{\alpha n\}$

* Partially supported by ONR Grant N00014-85-K-0368

to a certain set of matrices that is *almost* closed under multiplication.

2. DEFINITIONS. Let

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \tag{3}$$

so that

$$F^2 = F + I. \tag{4}$$

Then the set M^+ of all $cI + dF$ with positive determinant, and with c,d nonnegative integers, is a multiplicative semigroup. Call $c + d = n$ the *level* of a matrix in M^+. Since det(F) is negative, among the matrices of level n there is a unique one whose d is *maximal* and strictly less than n. We call this matrix μ_n, and we call the set $\{\mu_n\}$ the *edge* of M^+.

3. MULTIPLICATION OF EDGE ELEMENTS. If a large multiplication table is made of the μ_n, say for $1<n<100$, one observes that although the edge is not closed under multiplication, there is closure about 90 % of the time. What is the significance of this?

Let [x] denote the greatest integer in x, and set

$$a(n;\theta) = [\alpha n + \theta],\ a(n) = [n\alpha],\ \text{and}\ b(n) = [n\alpha^2]. \tag{5}$$

The functions a(n), b(n) are discussed at length in [2]. For a more general perspective, the reader may peruse

pp. 1-25 of [4] and the references at the end of [5].)

It is not hard to show that

$$\mu_n = \begin{vmatrix} 2n-a(n) & a(n)-n \\ a(n)-n & n \end{vmatrix} . \tag{6}$$

Now a proof of (1) can be based on the following identity, valid for integral n, K,L, and M:

$$a(Ka(n) + Ln + M) = Kb(n)+La(n)+a(M; (L\alpha - K)\{\alpha n\}/\alpha). \tag{7}$$

Here we use (7) for another purpose. Write

$$\mu_n \mu_m = (a_{ij}).$$

Is (a_{ij}) a matrix μ_ℓ in the edge? Observe that $a_{12}=a_{21}$ and $a_{11} + a_{12} = a_{22}$. Set

$$\ell = a_{11} + a_{12}. \tag{8}$$

Since

$$a_{11} = 2(a_{11} + a_{12}) - (a_{11} + 2a_{12}), \tag{9}$$

if

$$a(a_{22}) = a_{22} + a_{12} + h \tag{10}$$

then

(11) $a_{11} = 2\ell - a(\ell) + h$, $a_{12} = a(\ell) - \ell - h$, $a_{22} = \ell$,

and the answer is yes if and only if h=0. Next, define

(12) $c = a(M; (L\alpha - K)\{\alpha n\}/\alpha)$.

From (7) with $K = a(m) - m$, $L = 2m - a(m)$, and $M = 0$ we obtain

(13) $$\begin{aligned} a(a_{22}) &= a(2nm - na(m) - ma(n) + a(n)a(m)) \\ &= a(Ka(n) + Ln) = Kb(n) + La(n) + c \\ &= (a(m) - m)(a(n) + n) + (2m - a(m))a(n) + c \\ &= -nm + na(m) + ma(n) + c = a_{22} + a_{12} + c. \end{aligned}$$

But from $\alpha^2 = \alpha + 1$ one obtains

(14) $\theta = (L\alpha - K)\{\alpha n\}/\alpha = \alpha\{\alpha m\}\{\alpha n\} > 0$.

Thus h = c and the closure relation $\mu_n \mu_m = \mu_\ell$ is equivalent to $\theta < 1$, i.e.

(15) $$\{\alpha n\}\{\alpha m\} < \alpha^{-1}.$$

Since the region in [0,1] x [0,1] on which $xy < \alpha^{-1}$ has area A, where

(16) $$A = \frac{1}{\alpha} + 2\int_{1/\sqrt{\alpha}}^{1} (x\alpha)^{-1}\, dx = (\ell n(e\alpha))/\alpha = .9154392\ldots,$$

the "90 % closure" is explained. In fact, it can be shown that closure obtains if and only if n * m is in the range

of b, in which case

$$\mu_n \mu_m = \mu_{b^{-1}(n*m)} \tag{17}$$

(simply use $b(\ell) = 2a_{22} + a_{12} + h = (n*m) + h$).

Finally, we observe that in some sense the failure of closure is a virtue. Convert the multiplication table of $\{\mu_n\}$ to an infinite matrix of 0's and 1's by placing 1 wherever the product is a μ_ℓ, and 0 elsewhere. If r and s are rows (hence infinite 0-1 vectors) we say $r > s$ if in every column the element of r is at least as large as the element of s, and for some column the inequality is strict. Then the rows are totally linearly ordered, and every inequality between rows is strict! This follows from (15), and the irrationality of α. Hence all information about the *ordering* of the numbers $n\alpha$ modulo 1 is encoded in the "closure failures" of the edge of the semigroup. There are similar phenomena for other semigroup "edges", but we do not pursue this here.

REMARKS. The set of matrices

$$\begin{pmatrix} n & a(n) \\ a(n) & b(n) \end{pmatrix}$$

is a multiplicative semigroup. The edge of M^+ is an *approximate* semigroup in the sense that given μ_i and μ_j

one can find μ_k such that

$$\mu_i \mu_j - \mu_k$$

is bounded. For an interesting but negative result of this type, see Theorem 1 of [1].

We have found a host of identities between a(n) and b(n) that are not in [2]. For example.

$$b(b((a(n))^2 + (b(n))^2) = (a(b(n)))^2 + (b(b(n)))^2$$

and

$$a((a(n))^3 + 3n(a(n))^2 + n^3) = 2(a(n))^3 + 3n\, a(n)b(n).$$

We have been able to use some of them to show in an elementary way that the set

$$S_2 \cap [\emptyset\ S_2]$$

can be large. Here $\emptyset$ is a certain algebraic irrationality, and S_2 is the set of all integers of the form $x^2 + y^2$. Professors E. Fouvry and A. Schinzel remark that stronger results, valid for any irrational $\emptyset$, can be obtained using the deeper methods of H. Iwaniec; see [3].

ACKNOWLEDGEMENT. We thank Steven Skiena for computer generated data about these matrices. Also, Kenneth Stolarsky thanks Professor Vera Sós for stimulating discussions about the sequence $n\alpha$.

REFERENCES

[1] JOHN A. BAKER, The stability of the cosine equation, *Proc. Amer. Math. Monthly* 80(1980), 411-416.

[2] L. CARLITZ, V.E. HOGGATT, Jr., and R. SCOVILLE, Fibonacci representations, *Fib. Quart.* 10(1972), 1-28.

[3] H. IWANIEC, On indefinite quadratic forms in four variables, *Acta Arithmetica* 33(1977), 209-229.

[4] L. KUIPERS and H. NIEDERREITER, Uniform Distribution of Sequences, *John Wiley and Sons*, New York, 1974.

[5] KENNETH B. STOLARSKY, Beatty sequences, continued fractions, and certain shift operators, *Canad. Math. Bull.* 19(1976), 473-482.

PORTA, H. STOLARSKY, K.B.*

Department of Mathematics
University of Illionis
1409 West Green Street
Urbana, Illinois 61801
United States of America

* Partially supported by ONR Grant N00014-85-K-0368

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ARITHMETICAL TOPOLOGY

IMRE Z. RUZSA

1. ARITHMETIC, TOPOLOGY, AND ADDITIVE FUNCTIONS

For most of us, the integers form the par excellence discrete set. There are, however, other arithmetically important topologies on Z, the best known of which are the p-adic topologies. Other famous examples are Novoselov's polyadic topology and the Bohr topology. They are all well behaved topologies that give rise to beautiful compactifications. Rather pathetic topologies are also known to exist; Ajtai, Havas and Komlós [1] have shown that with a suitable topology Z turns into a topological group (with the operation of addition) that admits no continuous characters. (Their paper has strongly influenced this work.) Our aim is to demonstrate

that general questions concerning the possible topologies on Z may also lead to arithmetically relevant answers. This paper is intended to be an invitation to build a systematical theory of topologies on Z.

1.1 DEFINITION. By an *arithmetical topology* we mean any Hausdorff topology on Z, the set of integers, in which addition and substraction are continuous (that is, which turns Z into a topological group).

Convergence in a topology T will be denoted by $\xrightarrow{T}$.

Weaker or stronger requirements also make sense. For instance, we could impose the continuity of addition only (that is, consider Z as a topological semigroup), or we could also demand the continuity of multiplication, which would turn Z into a topological ring.

We consider the following question: under what conditions can a sequence of integers tend to 0 in an arithmetical topology?

1.2 DEFINITION. A sequence (a_n) of integers for which there is a group topology T on G such that $a_n \xrightarrow{T} 0$ will be called *nullpotent*.

The answer to our above question is connected with the equation

$$(1.3) \qquad n = \sum_{i=1}^{k} \varepsilon_i a_{j_i}, \quad \varepsilon_i = \pm 1 .$$

1.4 DEFINITION. We call the representation (1.3) *primitive*, if there is no nonempty subset $I \subset \{1,2,\ldots,k\}$, $I \neq 0$ of the subscripts such that

$$\sum_{i \in I} \varepsilon_i a_{j_i} = 0 .$$

THEOREM 1. *For any sequence* (a_i) *of integers the following are equivalent:*

(a) (a_i) *is a nullpotent sequence;*

(b) *for arbitrary integers* $k > 0$ *and* n, *the number of primitive solutions of* (1.3) *is finite;*

(c) *for arbitrary integer* $k > 0$ *and* $n \neq 0$, *there is a* $K = K(n,k)$ *such that in every solution of* (1.3) *we have* $j_i < K$ *for at least one* $1 \leq i \leq k$.

For example, $a_n = 2^n$ is a nullpotent sequence (it tends to 0 in the 2-adic topology), but $a_n = 2^n + 1$ is not, since $a_{n+1} - 2a_n = 1$; neither is $a_n = n^2$, since $a_{n+2} - 2a_{n+1} + a_n = 2$.

Besides a proof and generalizations of Theorem 1, we shall look for criteria for some concrete and random

sequences to be nullpotent. As an application, in §5 we find a new proof of Ajtai-Havas-Komlós' theorem quoted at the beginning.

The problem of nullpotent sequences arose out of another number theoretical problem concerning additive functions.

A classical theorem of Erdős [3] asserts that if a real valued additive arithmetical function f satisfies

$$f(n+1) - f(n) \to 0 \,, \tag{1.5}$$

then it must be of the form $f(n) = c \log n$. Since then, scores of variants apperared. Recently E. Wirsing (unpublished) proved the following deep generalization. If f is an additive function and

$$f(n+1) - f(n) \to 0 \pmod 1,$$

then $f(n) \equiv c \log n \pmod 1$. In other words, if a complex valued multiplicative function h satisfies

$$|h(n)| = 1,\ h(n+1) - h(n) \to 0 \,,$$

then $h(n) = n^{ic}$ with a suitable real c. This inspired Daróczy and Kátai [2] to investigate the following. Let G be a commutative topological group (written additively), and $f: N \to G$ a G-valued additive arithmetical function. Assume (1.5) (where '0 is the zero element of G). Does it

follow that f is the restriction of a continuous homomorphism $\varphi:(0,\infty)\to G$, where the operation on the positive halfline is the multiplication? They provide the affirmative answer for the case when G is a compactly generated locally compact group.

The idea in Daróczy and Kátai's work is to apply Wirsing's theorem to the functions $\gamma(h(n))$, where γ runs over the characters of G. This approach definitely does not extend beyond the class of group that are separated by their characters. This observation and the result of Ajtai, Havas and Komlós led me to the following problem. Is there an integer-valued additive function f, $f \not\equiv 0$, and an arithmetical topology T such that

$$(1.6) \qquad f(n+1) - f(n) \xrightarrow{T} 0 \ ?$$

This immediately leads to the problem about the description of nullpotent sequences. The answer given by Theorem 1 does reduce (1.6) to a purely arithmetical problem, but does not immediately yield a solution.

A further discussion of this problem, including the construction of a solution of (1.6), will be given in a joint paper by R. Tijdeman and the author.

PROBLEMS. 1) Given a sequence, when does an arithmetical topology exist in which this sequence is a) convergent, b) a Cauchy sequence?

2) Given a set A of integers, when does an arithmetical topology exist in which this set is a) closed (or open), b) everywhere dense?

2. THEOREM 1: A METRIC PROOF

Theorem 1 easily generalizes to all commutative groups. In the sequel, let G be a commutative group, written additively (correspondingly the neutral element will be denoted by 0).

2.1 DEFINITION. A Hausdorff topology on G that turns G into a topological group will be called a *group topology*.

2.2 DEFINITION. A sequence (a_n) of elements of G for which there is a group topology T on G such that $a_n \xrightarrow{T} 0$ will be called *nullpotent*.

The description of nullpotent sequences is connected with the equation

$$g = \sum_{i=1}^{k} \varepsilon_i a_{j_i}, \quad \varepsilon_i = \pm 1 . \tag{2.3}$$

The *primitivity* of a representation (2.3) is defined exactly as in Definition 1.4.

THEOREM 1A. *For any sequence* (a_i), $a_i \in G$, *the following are equivalent:*

(a) (a_i) *is a nullpotent sequences;*

(b) *for arbitrary integer* $k > 0$ *and* $g \in G$, *the number of primitive solutions of* (2.3) *is finite;*

(c) *for arbitrary integer* $k > 0$ *and* $0 \neq g \in G$, *there is a* $K = K(n,k)$ *such that in every solution of* (2.3) *we have* $j_i \leq K$ *for some* $1 \leq i \leq k$.

Moreover, if these conditions are satisfied, then the group topology in which $a_i \to 0$ *can be chosen to be metrizable.*

PROOF. (a) → (c). Let U be a symmetric neighbourhood of 0 such that $g \notin kU$. (By kU we mean the algebraic sum

$$kU = U + U + \ldots + U, \quad k \text{ summands}).$$

We have $a_i \in U$ for $i > K$. Now if in (2.3) every subscript is $> K$, then the right side is in kU while the left side is not.

(c) → (b). We proceed by induction on k. For $k = 1$, the statement is obvious: the only suffix is at most $K(g, 1)$ (if $g = 0$, then, by definition, the representation cannot be primitive).

Assume we know statement (b) for k-1 in the place of k and every g. One of the suffices, say j_m, is at most $K(g, m)$. (2.3) can be rewritten as

$$g-\varepsilon_m a_{j_m} = \sum_{\substack{i=1 \\ i\neq m}}^{k} \varepsilon_i a_{j_i} .$$

For a fixed choice of ε_m and j_m, this has a finite number of solutions by the induction hypothesis; since the number of possible equations is also finite, so is the total number of solutions.

The proof of (b) → (a) will be more complicated.

2.4 DEFINITION. By a *seminorm* on G we mean a real-valued function $N:G\to R$ such that

$$N(x) \geq 0,\ N(-x) = N(x),\ N(x+y) \leq N(x) + N(y)$$

for all $x,y\in G$. A seminorm is a *norm* if $N(x) > 0$ unless $x = 0$.

A norm obviously defines a metric topology.

Any nonnegative function $H:G\to[0,\infty)$ induces a seminorm $N = N_H$ in the following way:

$$N_H(g) = \inf \{H(x_1) + \ldots + H(x_k):$$

$$\varepsilon_1 x_1 + \ldots + \varepsilon_k x_k = g,\ \varepsilon_i = \pm 1,\ k=1,2,\ldots\}.$$

This is always a seminorm and satisfies $N_H(x) \leq H(x)$ for all $x\in G$.

Now for a fixed sequence (a_i) satisfying (b) and any $0 \neq g \in G$ we are going to define a seminorm N_g such that

$$N_g(g)=1,\ N_g(x)\leq 1 \text{ for all } g\in G,\ N_g(a_i)\to 0 \text{ as } i\to\infty .$$

We first define $H(x)$ as follows. If $x \notin \{a_i\}$, let $H(x)=1$. If $x = a_i$, consider all the primitive solutions of (2.3) in which a_i occurs. If there is no such solution, we put $H(x)=0$. If there are solutions and the minimal value of k in them is k_0, we put $H(x)=1/k_0$.

We have $H(a_i)\to 0$, since any fixed value $1/k$ occurs only at the finite set of suffices that figure in the finitely many primitive solutions of (2.3).

Writing $N_g(x)=N_H(x)$, the inequality $N_H \leq H$ implies

$$N_g(x) \leq 1,\ N_g(a_i) \to 0 .$$

We have yet to show $N_g(g) = 1$.

Consider any sum

$$s = \Sigma\ H(x_i),\ g = \varepsilon_1 x_1 + \ldots + \varepsilon_k x_k .$$

If any x_i is outside the set $\{a_j\}$, then we have $s \geq H(x_i) = 1$.

If all are in this set, say $x_i = a_{j_i}$, and the representation is primitive, then we have $H(a_i) \geq 1/k$ for all i.

Finally, if the representation is not primitive, the select a minimal set $J \subset \{1, \ldots, k\}$ such that

$$g = \sum_{i \in J} \varepsilon_i a_{j_i} .$$

This representation must already be primitive, thus we can again conclude

$$s \geq \sum_{i \in J} H(x_i) \geq 1 .$$

Now let $B = \{b_1, b_2, \ldots\}$ be the set of all elements of G that have a representation of the form (2.3); this is clearly a countable set. Obviously for any of the norms N_g we have $N_g(x) = 1$ if $x \in B$. Put

$$N(x) = \sum_{i=1}^{\infty} 2^{-i} N_{b_i}(x) .$$

Since the series is uniformly convergent, this defines a seminorm. It actually will be a norm, since

$$N(b_i) \geq 2^{-i} N_{b_i}(b_i) = 2^{-i}, \quad N(x) = 1 \text{ if } x \notin B .$$

Finally, since $N_{b_i}(a_j) \to 0$ as $j \to \infty$ for any fixed i and the series is uniformly convergent, we have $N(a_j) \to 0$. This amounts to $a_j \to 0$ in the topology induced, qu. e.d.

This proof is similar to the construction of Ajtai-Havas-Komlós [1].

3. CRITERIA FOR NULLPOTENCY

As Theorem 1 indicates, the property of nullpotency is a deep additive one which may be difficult to decide for a simple arithmetically defined sequence. In fact, the only general condition I know is the following.

3.1 STATEMENT. *If* $a_{n+1}/a_n \to \infty$ *as* $n \to \infty$, *then the sequence* (a_n) *is nullpotent.*

PROOF. We consider the equation 1.3 . Let K be such that $a_{i+1}/a_i > 2k$ and $a_i > 2|n|$ for $i > K$. Let J be the largest subscript j_i (after the possible cancellations). If $j > K$, then we have

$$|n| > a_j - (k-1)a_{j-1} > a_j/2 > |n| ,$$

a contradiction. We conclude $j_i \leq K$, and the nullpotency of our sequence follows from Theorem 1, (c).

A necessary condition is given by the following result.

THEOREM 2. *Let* (a_i) *be a nullpotent sequence of integers and let* B_i *be the set of integers* n *that can be written in the form* (1.3). *For every* k, B_i *has asymptotical denseity* 0. *In particular, an asymptotical basis is never nullpotent.*

Recall that a set A is an asymptotical basis of order h if hA contains all but a finite number of positive integers.

PROOF. We use induction on k. For k = 0 the statement is obvious ($B_0 = \{0\}$).

Assume we know the statement for k-1. Choose a positive ε and an integer m with $\varepsilon m > 1$. Choose an arithmetical topology in which $a_i \to 0$ and a neighbourhood U of 0 such that

$$U \cap \{1, 2, \ldots, m\} = 0 \quad . \tag{3.2}$$

Let V be a neighbourhood of 0 with $V - V \subset U$. By (3.2), V can contain at most one out of any collection of m consecutive integers; in particular, we have

$$\bar{d}(V) \leq 1/m < \varepsilon \quad .$$

Take now a symmetric neighbourhood W of 0 such that $kW \subset V$. We have $a_i \in W$ for $i > K$.

We split the elements of B_k into two classes, $B_k = C \cup D$. In C we put those elements in whose representation (1.3) some of the subscripts is $j_i \leq K$; those for which $j_i > K$ for all i get into D. Since these a_i's ($i > K$) are in W, we have

(3.3) $\quad D \subset kW \subset V,\ \bar{d}(D) \leq \bar{d}(V) < \varepsilon\ .$

On the other hand, we have

$$C \subset \{a_1, -a_1, \ldots, a_K, -a_K\} + B_{k-1},$$

thus

(3.4) $\quad \bar{d}(C) \leq 2Kd(B_{k-1}) = 0$

by the induction hypothesis. (3.3) and (3.4) together imply $\bar{d}(B_k) < \varepsilon$; sinc ε was arbitrary, we conclude $d(B_k) = 0$.

REMARK. It may seem somewhat perverse that to deduce such an arithmetical property we used the topological concept rather than the arithmetical conditions given under (b) and (c) of Theorem 1. These seem to offer no easier approach.

Finally, we give a nontrivial example of a nullpotent sequence.

THEOREM 3. *Let* P *be a finite set of primes and let* (a_i) *be the sequence of positive integers composed exclusively of primes belonging to* P. *The sequence* (a_i) *is nullpotent.*

For the proof, we need a deep result of Evertse (Corollary 1 of [5]), which we quote with some change

of notation.

3.5 LEMMA. *Let* c, d *be constants with* c>0, 0≤d<1, *let* P *be a finite set of primes and let* k *be a positive integer. There are only finitely many tuples* $(x_0, x_1, \ldots, x_k)$ *of integers such that*

$$x_0 + \ldots + x_k = 0, \tag{3.6}$$

$$\sum_{i=I} x_i \neq 0 \tag{3.7}$$

for every proper nonempty subset $I \subset \{0, 1, \ldots, k\}$,

$$\gcd(x_0, \ldots, x_k) = 1 , \tag{3.8}$$

$$\prod_{i=0}^{k} \left(|x_i| \prod_{p \in P} |x_i|_p \right) \leq c(\max x_i)^d . \tag{3.9}$$

Here $|x|_p$ is the p-adic norm, that is, if $x = p^j m$ with p|m, then $x_p = p^{-j}$.

PROOF of Theorem 3. Call a solution of (1.3) *superprimitive*, if it is primitive and the gcd of the terms a_{j_i} is 1.

First we show that the number of superprimitive solutions is finite. Given a solution of (1.3), write

$$x_0 = -n, \quad x_i = \varepsilon_i a_{j_i} \quad (i=1,\ldots,k) .$$

This will be a solution of (3.6), while superprimitivity guarantees (3.7) and (3.8). Since for $i > 0$ $x_i = a_{j_i}$ is composed exclusively of primes of P, we have

$$|x_i| \prod_{p \in P} |x_i|_p = 1 \quad (i \geq 1) .$$

This shows that (3.9) holds with $c = n$ and $d = 0$; an application of Lemma 3.5 yields the finiteness of superprimitive solutions.

Observe that by dividing a primitive representation (1.3) by

$$d = \gcd (a_{j_1}, \ldots, a_{j_k})$$

we obtain a superprimitive representation of $n' = n/d$. Since the number of possible values of n' as well as the number of solutions for each n' are finite, the finiteness of the total number of primitive solutions of (1.3) follows. By virtue of Theorem 1 we conclude that the sequence is nullpotent.

REMARK. The quoted result of Evertse is "unnecessarily" strong; for our purposes probably some earlier weaker result would equally suffice. In fact, the same proof yields the following stronger version of Theorem 3.

THEOREM 3A. *Let* P *be a finite set of primes and let* (a_i) *be a sequence of positive integers. Assume that* $a_i = b_i c_i$, *where* b_i *is composed exclusively of primes belonging to* P *and the integers* c_i *satisfy* $c_i = 0(a_i^{\varepsilon})$ *for every* $\varepsilon > 0$ *as* $i \to \infty$. *The sequence* (a_i) *is nullpotent.*

PROBLEMS. 1) Which linear recurrence sequences are nullpotent? *Conjecture:* a linear recurrence sequence is nullpotent unless there is a root of unity among the roots of the characteristic polynomial.

2) Is there an infinite set P of primes such that the sequence of integers composed only of primes belonging to P is nullpotent?

3) Let B_k be as in Theorem 2, and let $B_k(x)$ denote the number of elements of B_k in $[1, x]$. Is it true that

$$B_{k+1}(x)/B_k(x) \to \infty \ ?$$

The same can be asked for the set A_k of sums of k terms (without the coefficients ± 1). For k=1 both are easily proved.

4. NULLPOTENCY OF RANDOM SETS

We have observed that any sequence with $a_{n+1}/a_n \to \infty$ must be nullpotent, while an exponential one like 2^n+1 may not. However, "typically" any thinner than polynomial sequence is nullpotent. This can be expressed in probabilistic terms. Let (ξ_n) be a sequence of independent 0-1 valued random variables with

$$P(\xi_n = 1) = p_n \quad .$$

We define a random set A by

$$A = \{n:\xi_n = 1\} \quad ;$$

then the events $n \in A$ will be independent of each other and

$$P(n \in A) = P(\xi_n = 1) = p_n \ .$$

THEOREM 4. *Let p_n be a sequence of real numbers such that*

$$(4.1) \qquad 0 \le p_n \le 1, \ \Sigma p_n = \infty, \ p_n = 0(n^{-(1-\varepsilon)})$$

for every $\varepsilon > 0$. The random set A defined above will be nullpotent with probability 1.

REMARK. In (4.1), $\Sigma p_n = \infty$ guarantees that A will be infinite with probability one. According to the law of large numbers, the last inequality of (4.1) means that with probability 1 we have

$$\#\{n \in A : n \le x\} = \sum_{n \le x} \xi_n \sim \sum_{n \le x} p_n = O(x^{\varepsilon}) .$$

PROOF. According to Theorem 1, A is nullpotent if and only if for every fixed n and k the equation

$$(4.2) \qquad n = \varepsilon_1 x_1 + \ldots + \varepsilon_k x_k, \ \varepsilon_i = \pm 1$$

has only a finite number of primitive solutions with $x_i \in A$.

By collecting the equal terms and reordering, (4.2) can be rewritten as

$$(4.3) \qquad n = b_1 x_1 + \ldots + b_m x_m, \ \Sigma |b_i| \le k, \ x_1 < \ldots < x_m, \ b_i \neq 0 .$$

For a fixed k, the number of possible tuples $(b_1, \ldots, b_m)$ is finite, thus it is sufficient to show that for fixed n and b_i, (4.3) has, with probability one, only a finite number of solutions.

Select an $\varepsilon < 1/m$. For a fixed system $(x_1, \ldots, x_m)$ the probability that they are all in A is

$$p_{x_1} \ldots p_{x_m} \le C(\varepsilon)\ (x_1 \ldots x_m)^{-(1-\varepsilon)} \le$$

$$\le C(x_1 \ldots x_{m-1})^{-(1-\varepsilon)m/(m-1)} .$$

We write Σ' to denote that the summation is over the solutions of (4.3). For given $x_1, \ldots, x_{m-1}$ there is at most one x_m to satisfy (4.3), thus we have

$$\Sigma' P(x_1 \in A, \ldots, x_m \in A) \le C\Sigma' (x_1 \ldots x_{m-1})^{-(1-\varepsilon)m/(m-1)}$$

$$\le C \sum_{x_1=1}^{\infty} \ldots \sum_{x_{m-1}=1}^{\infty} (x_1 \ldots x_{m-1})^{-(1-\varepsilon)m/(m-1)} < \infty$$

since $(1-\varepsilon)m/(m-1)>1$. By the Borel-Cantelli lemma, with probability one there are only finitely many solutions.

REMARK. In contrast to Theorem 4, if we put $p_n = cn^{-d}$ with a fixed constant $d<1$, then with probability one A will be an asymptotical basis and hence not nullpotent by Theorem 2. The fact that A will be a basis can be shown by the methods of Erdős and Rényi [4], and also easily follows from their Theorem 6. I do not know of any explicite formulation of this statement, and, since the proofs given in [4] are somewhat sketchy, it may be of some interest to give a detailed proof; but this lies definitely outside the scope of this paper.

In the previous section we observed that a nullpotent sequence cannot be a basis. However, it can be an essential component. If we make a random set A with $p_n=(\log n)^3/n$, then with probability one it will be nullpotent by Theorem 4. It will also be an essential component, even with the stronger property that $d(A+B)=1$ for every set B with $\underline{d}(B)>0$; see Ruzsa [6].

5. CHARACTER BUSTING

Ajtai, Havas and Komlós [1] show that there is an arithmetical topology with no continuous characters in the following way. They find a nullpotent sequence (a_n) such that

$$\gamma(a_n) \not\to 1 \tag{5.1}$$

for every nonprincipal character γ of N. They do this by a "semirandom" construction: they choose randomly one number from each of the intervals

$$[u_n, v_n], \ u_n = 2^{[n^{1/2}]}, \ v_n = u_n + 2^{[n^{1/3}]} .$$

This sequence has $\sim c(\log x)^2$ elements up to x.

A "purely random" variant is the following. Select the integers n into A independently of each other with probability

$$p_n = c \frac{\log n}{n}$$

(this yields the same order of magnitude for A). The set A is nullpotent with probability one by Theorem 4, and also satisfies (5.1) with probability one; this can be shown analogously to the proof in [1].

A deterministic construction can also be given. Put

$$a_{2n} = 2^n, \; a_{2n+1} = 3^n .$$

The nullpotency of this sequence follows from Theorem 3. To show (5.1), observe that the characters of N are the functions

$$\gamma(n) = e^{i\alpha n}, \quad \alpha \in R .$$

(5.1) can be rewritten as

$$\|\alpha a_n\| \not\to 0 ,$$

where $\|x\| = \min(\{x\}, 1-\{x\})$ is the distance of x from the nearest integer. Now $\|2^n\alpha\| \to 0$ means that α is a diadic rational, while $\|3^n\alpha\| \to 0$ means it is a triadic one, and if it is both, it must be an integer, hence γ is the

principal character.

The price we had to pay for this simple proof is the application of Theorem 3, which is based on deep results from diophantine analysis.

Our sequence arose as the union of two simple sequences. The following questions pop up naturally.

(i) Is the union of two nullpotent sequences always nullpotent? The answer is naturally no; both n! and n!+1 are nullpotent, while their union is not. One can construct m+1 sequences with the property that the union of any m of them is nullpotent, but the union of all m+1 is not. For instance, let

$$a_i^{(j)} = (im+j)!,\ j-1,\ \ldots,\ m\ ;$$

$$a_i^{(0)} = a_i^{(1)} + \ldots + a_i^{(m)} + 1\ .$$

(ii) $2^n \to 0$ in the 2-adic topology, $3^n \to 0$ in the 3-adic one; is it possible to combine the two and to obtain a topology in which both tend to 0 immediately? This question is somewhat vague, and I feel the answer is anyway negative. If we interpret it as "find a topology, in which every sequence tends to 0 that does so in the 2-adic or 3-adic topology", then a negative answer is easily given. (Hint: find b_n and c_n so that

$$2^n | b_n,\ 3^n | c_n,\ b_n + c_n = 1.)$$

PROBLEM. On which commutative groups is there a group topology in which no character is continuous?

6. SIMULTANEOUS NULLPOTENCY

We investigate the following question: given a collection of sequences, when does an arithmetical topology exist in which they all tend to 0. We have already observed that the nullpotency of each of the sequences is insufficient. Now we investigate infinite systems; we shall find a certain "countable compactness".

THEOREM 6. *Let* $A_k=(a_i^{(k)})$, $k=1,2,\ldots$ *be a collection of sequences of integers. If the union* $A_1\cup\ldots\cup A_m$ *is nullpotent for every* m, *then there is a nullpotent sequence* A *that contains every* A_k *except a finite number of elements; consequently, there is an arithmetical topology in which* $a_i^{(k)}\to 0$ *for every* k *as* $i\to\infty$.

On the other hand, there is a collection $B_t=(b_i^{(t)})$ *of sequences,* $0<t<1$, *with the property that the union of any finite number of them is nullpotent, but there is no arithmetical topology in which* $b_i^{(t)}\to 0$ *for every* t.

PROOF. We start with the countable case. Let (n_j, k_j), $j=1, 2, \ldots$ be an enumeration of all pairs of positive integers. For an arbitrary pair $m>j\geq 1$ of

integers, consider the primitive representations of n_j with k_j elements of $A_1 \cup \ldots \cup A_m$, with coefficients ± 1. By assumption, the number of these representations is finite, thus there is a maximal one among the suffices i for which $a_i^{(m)}$ occurs in one of them; denote it by M(j, m). Put

$$M(m) = \max_{j<m} M(j, m)$$

Now let $A=\{a_1, a_2, \ldots\}$ be a sequence containing, in some order, all the integers $a_i^{(j)}$, $i>M(j)$. We claim that A is nullpotent.

Take a pair (n, k) of integers; this pair occurs in our enumeration, say $n=n_q$, $k=k_q$. We investigate the equation (1.3). Instead of $a_i^{(j)}$ let us write a(i, j). By substituting a suitaible a(i, j) for each element of A and rearranging, a representation of n by k terms can be written as

$$n = \varepsilon_i a(i_1, u_1)+\ldots+\varepsilon_k a(i_k, u_k), \quad \varepsilon_j=\pm 1,$$

$$i_j>M(u_j), \quad u_1\leq\ldots\leq u_k \ .$$

We assert $u_k \leq q$; otherwise we would have

$$i_k \leq M(q, u_k) \leq M(u_k) < i_k \ ,$$

a contradiction.

Now assume that there is a topology T in which

$$[g(n+t)] \to 0 \quad \text{as} \quad n \to \infty$$

for all $t \in (0, 1)$. Take a neighbourhood U of 0 in T such that $1 \notin U-U$. This means that from two consecutive integers n and n+1 at most one can be inside U.

We define recursively a nested sequence of closed intervals

$$I_k = [u_k, v_k] \subset (0, 1), \; I_{k+1} \subset I_k, \; k=1,2,\ldots$$

with the properties that

$$M_k = g(k+u_k) \quad \text{is an integer;}$$

$$g(k+v_k) = M_k + 1/2;$$

$$M_k \notin U \; .$$

I_1 can be found with $M_1 = 4$ or 5. Assume we have I_k; we define I_{k+1}. With $M = M_k$ we have

$$g(k+1+u_k) = M^2, \; g(k+1+v_k) = (M+1/2)^2 = M^2+M+1/4 \; .$$

Put $N = M^2$ if $M^2 \notin U$, $N = M^2 + 1$ if $M^2 \in U$ and define I_{k+1} by

$$g(k+1+u_{k+1}) = N, \; g(k+1+v_{k+1}) = N + 1/2 \; .$$

We obtained $u_j \le u_k \le q$ for all j, therefore all the terms are from $A_1 \cup \ldots \cup A_q$; now the finiteness of the number of solutions follows from the assumption.

This concludes the proof of the first part.

We turn to the second assertion of the theorem. Write $g(x)=2^{2^x}$; we put

$$b_n^{(t)} = [g(n+t)], \quad 0<t<1, \quad n=1,2,\ldots .$$

First we show that any finite union of these sequences is nullpotent. Let $t_1, \ldots, t_k \in (0, 1)$ be k different numbers and let

$$B = \{b_1<b_2<\ldots\} = B_{t_1} \cup \ldots \cup B_{t_k} .$$

Write

$$\delta = \min_{i \neq j} \| t_i - t_j \| .$$

Two consecutive elements of B are of the form

$$b_r = [g(m+t_i)], \quad b_{r+1} = [g(n+t_j)] \quad (n=m \text{ or } m+1) .$$

We have $n+t_j \ge m+t_i+\delta$, therefore

$$b_{r+1} \ge \left[b_r^{1+\delta}\right], \quad b_{r+1}/b_r \to \infty ,$$

and B is nullpotent by Statement 3.1.

This satisfies all our requirements. Finally, if

$$\bigcap_{k=1}^{\infty} I_k = \{\beta\} ,$$

then we have

$$b_k^{(\beta)} = [g(k+\beta)] = M_k \notin U$$

for every k, thus 0 is not even a cluster point of the sequence B_β in T.

PROBLEM. Find a criterion for the existence of an arithmetical topology in which a given (uncountable) family of sequences can all simultaneously tend to 0.

7. THEOREM 1. A GENERALIZATION TO NETS

We give a proof of Theorem 1 that constructs the topology directly rather than via a norm. I feel that this is the "real" proof, which is shown by the fact that it will generalize to nets while the metric proof obviously cannot. The importance of this is that the convergence of sequences is insufficient to describe a topology unless it is first countable. Nets are sequence-like things with subscripts from a general directed set

rather than from the positive integers; for an exact definition and basic properties we refer the reader to Kelley [5].

Let G be a commutative group, J a directed set, $(g_j)_{j\in J}$ a net of elements of G.

7.1 DEFINITION. A net (a_j) of elements of G for which there is a group topology T on G such that $a_j \xrightarrow{T} 0$ will be called *nullpotent*.

Nullpotency is connected with the equation

$$g = \sum_{i=1}^{k} \varepsilon_i a_{j_i}, \quad \varepsilon_i = \pm 1, \ j_i \in J \ . \tag{7.2}$$

THEOREM 1B. *The following are equivalent:*

(a) *the net* (a_i) *is nullpotent;*

(b) *for arbitrary integer* $k>0$ *and* $g\in G$ *there is a* $j'\in J$ *such that* (7.2) *has no solution with*

$$j_1 > j', \ \ldots, \ j_k > j' \ .$$

For I = {positive integers} this reduces to Theorem 1A.

The implication (a) → (b) can be shown in the same way as in §2. We prove (b)→(a).

Let S be the set of infinite sequences v of elements of J

$$v = (v_1, v_2, \ldots), \; v_i \in J .$$

For every $v \in S$ we define a set $U_v \subset G$ as follows. U_v is the set of all elements g of G that can be represented with some integer k in the form

$$\varepsilon_1 a_{j_1} + \ldots + \varepsilon_k a_{j_k}, \; \varepsilon_i = \pm 1, \; j_i \in J, \; j_i > v_i .$$

We take the collection of sets $\{U_v\}$ as a basis of neighbourhoods at 0. To see that it can serve as a basis we have to check the following:

(1) for every $v \in S$ and $g \in U_v$ there is a $w \in S$ such that $g + U_w \subset U_v$ (openness);

(2) for every $v \in S$ there is a $w \in S$ such that $U_w - U_w \subset U_v$ (compatibility with the operation);

(3) for every $g \neq 0$ there is a $v \in S$ such that $g \notin U_v$ (Hausdorff separation axiom).

(1) and (2) hold for every net (a_i); we need (c) only to prove (3).

Proof of (1). Let

$$g = \varepsilon_1 a_{j_1} + \ldots + \varepsilon_k a_{j_k},\ j_1 > \nu\ ,\ \ldots,\ j_k > \nu_k\ .$$

Put $w = (\nu_{k+1},\ \nu_{k+2},\ \ldots)$; with this choice we have $g + U_w \subset U_\nu$.

Proof of (2). For every k take a $w_k \in J$ so that

$$(7.3) \qquad w_k > u_1,\ w_k > u_2,\ \ldots,\ w_k > u_{2k}\ .$$

Let $w = (w_1,\ w_2,\ \ldots)$. It is easy to check that $U_w - U_w \subset U_\nu$.

Proof of (3). Take a $g \neq 0$. For every k there is a $j' = j'(k)$ such that g has no representation (7.2) with $j_i > j'(k)$ for all $i=1,\ldots,k$. Putting

$$\nu = (j'(1),\ j'(2),\ \ldots)$$

this ensures $g \notin U_\nu$.

This finishes our proof that this defines a group topology. We show that $a_j \to 0$ in this topology. Take an arbitrary neighbourhood U of 0. By definition, there is an

$$U_v \subset U,\ v \in S,\ v = (v_1, v_2, \ldots) .$$

By definition, we have

$$a_j \in U_v \subset U$$

for $j > v_1$.

PROBLEM. Generalize Theorems 1A-1B to noncommutative groups.

REFERENCES

[1] M. AJTAI, I. HAVAS, J. KOMLÓS, 'Every group admits a bad topology', in: *Studies in pure mathematics to the memory of P. Turán*, ed. P. Erdős, Birkhäuser, 1983, p. 21-34.

[2] Z. DARÓCZY, I. KÁTAI, On additive arithmetical functions with values in topological groups I., Publ. Math. Debrecen 33 (1986), 287-291.

[3] P. ERDŐS, 'On the distribution function of additive functions', *Annals of Math.* 47 (1946), 1-20.

[4] P. ERDŐS, A. RÉNYI, 'Additive properties of random sequences of positive integers', *Acta Arith.* 6 (1960), 83-110.

[5] J. L. KELLEY, *'General topology'*, Van Nostrand, Princeton 1955.

[6] I. Z. RUZSA, 'Probabilistic constructions in additive number theory', Astérisque 147-148 (1987) 173-182 (Proc. of the Journées Arithmétiques, Besançon 1986).

Imre, Z. RUZSA

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Pf. 127.
H-1364 H u n g a r y

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ASYMPTOTIC DISTRIBUTIONS OF DIGITS IN INTEGERS

IEKATA SHIOKAWA

For an increasing sequence of positive integers $n_1, n_2, \ldots$, let $A(x)$ be the number of n_i's up to x. Copeland and Erdős [1] proved that if, for any $\varepsilon > 0$,

$$A(x) > x^{1-\varepsilon} \tag{1}$$

provided that x is sufficiently large, or what amounts the same thing

$$\log \frac{x}{A(x)} = o(\log x)$$

as $x \to \infty$, then the infinite decimal $0.n_1n_2\ldots$ is normal to base r when each of these integers n_i is replaced by its r-adic expansion. In the present paper we shall refine this results and make some remarks on it.

1. STATEMENTS OF RESULTS

Throughout of this paper r is an integer greater than 1. Every positive integer n can be written uniquely as

$$(2) \qquad n = a_1 a_2 \ldots a_k = \sum_{i=1}^{k} a_i r^{k-i},$$

where each a_i is one of $0,1,\ldots,r-1$, and $a_1 \neq 0$, or equivalently $k = [\log_r n] + 1$, where $[t]$ is the greatest integer not exceeding a real number t. For any sequence $b_1, b_2, \ldots, b_l$ of 0's, 1's, ..., and r-1's of length l, we denote by $N(n) = N_r(n; b_1 b_2 \ldots b_l)$ the number of indices i's in the expression (2) such that $a_i = b_1, a_{i+1} = b_2, \ldots, a_{i+l-1} = b_l$. We put $s_r(n) = \sum_{i=1}^{k} a_i$, so that

$$(3) \qquad s_r(n) = \sum_{b=1}^{r-1} b N_r(n;b)$$

THEOREM 1. *Let $n_1, n_2, \ldots$ be any, finite or infinite, increasing sequence of positive integers. Then, for any l integers $b_1, b_2, \ldots, b_l$ with $0 \leq b_i < r$, we have*

$$\Big| \sum_{n_i \le x} N_r(n_i; b_1 b_2 \dots b_l) - \frac{1}{r^l} A(x) \log_r x \Big|$$

$$\le c \max_{y \le x} \left(\frac{\log \frac{y}{A(y)} + \log(\log_{r^l} y)}{\log_{r^l} y} \right)^{\frac{1}{2}} A(y) \log_{r^l} y ,$$

provided $x \ge r^{lr^{2l}}$, *where* $c = 2^8 l$.

By the relation (1) we have the following

COROLLARY 1. (cf. Heppner [2]). *For any, finite or infinite, increasing sequence* $n_1, n_2, \dots$ *of positive integers, we have*

$$\Big| \sum_{n_i \le x} s_r(n_i) - \frac{r-1}{2} A(x) \log_r x \Big|$$

$$\le c_1 \max_{y \le x} \left(\frac{\log \frac{y}{A(y)} + \log(\log_r y)}{\log_r y} \right)^{\frac{1}{2}} A(y) \log_r y ,$$

provided $x \ge r^{r^2}$, *where* $c_1 = 2^7 r(r-1)$.

Example 1. Let $\varphi(n)$ be the Euler function. Then we obtain

$$\sum_{\substack{m \le n \\ (m,n)=1}} s_r(m) = \left(1 + 0\left(\frac{\log \log n}{\log n} \right)^{\frac{1}{2}} \right) \frac{r-1}{2} \varphi(n) \log_r n ,$$

using the estimates $\liminf_{n \to \infty} \varphi(n)(\log \log n)/n > 0$.

Example 2. (Shiokawa [9], Heppner [2]).

$$\sum_{p\le x} s_r(p) = \left(1 + 0\left(\frac{\log\log x}{\log x}\right)^{\frac{1}{2}} \frac{r-1}{2} \frac{x}{\log r}\right),$$

where p runs through prime numbers. This result was considerably improved by Kátai [4]. Indeed, he proved the following inequality

$$\sum_{p\le x} \left|s_r(p) - \frac{r-1}{2}\frac{x}{\log r}\right|^k = O(x(\log x)^{k/2-1}) \quad (k=1,2,\ldots).$$

Every irrational number θ with $0 \le \theta < 1$ can be uniquely expanded to base r as

$$(4) \qquad \theta = 0.a_1a_2\ldots = a_1r^{-1} + a_2r^{-2} + \ldots ,$$

where each a_i is one of $0,1,\ldots,r-1$. Then θ is said to be normal to base r, if the relative frequency $t^{-1}N(t;\theta;b_1b_2\ldots b_l)$ of a given sequence $b_1,b_2,\ldots,b_l$ as in Theorem 1 tends to r^{-l} as $t\to\infty$, where $N(t;\theta;b_1b_2\ldots b_l)$ is the number of occurrences of the sequence $b_1b_2\ldots b_l$ in the first t digits $a_1a_2\ldots a_t$. Let $n_1,n_2,\ldots$ be any increasing sequence of positive integers and let $n_j = a_{j1}a_{j2}\ldots a_{jk_j}$ be the expression (2) of n_j. We define by (4) a number $\theta_r = 0.a_{11}a_{12}\ldots a_{1k_1}\ a_{21}\ldots a_{2k_2}\ldots$, which will be written simply as $\theta_r = 0.n_1n_2\ldots$. Then Copeland and Erdős proved that, for any increasing sequence $n_1,n_2\ldots$ of positive integers satisfying (1),

$t^{-1}N(t;\theta_r;b_1b_2\ldots b_l) = r^{-l} + o(1)$ as $t \to \infty$. It seems difficult, in general, to estimate the remainder $o(1)$ explicitly in terms of t. However, choosing an index $i = i(t)$ such that

$$\sum_{h=1}^{i-1} [\log_r n_h + 1] \le t < \sum_{h=1}^{i} [\log_r n_h + 1] ,$$

we have the following

THEOREM 2. *Let* $n_1, n_2, \ldots$ *be any increasing sequence of positive integers satisfying* (1). *Then, for any* $b_1, b_2, \ldots, b_l$ *as in Theorem 1, we have*

$$\frac{N(t)}{t} = \frac{1}{r^l} + O\left\{\left(\frac{\log \frac{n_{i(t)}}{i(t)} + \log\log t}{\log t}\right)^{\frac{1}{2}}\right\} ,$$

where $\log(n_{i(t)}/i(t)) = o(\log t)$ *as* $t \to \infty$ *and the constant implied depends possibly on* r *and* l.

Example 3. Let $\theta_r = 0.23571113\ldots$ be the number defined by the sequence of primes. Then

$$\frac{1}{t} N(t;\theta_r;b_1b_2\ldots b_l) = \frac{1}{r^l}\left\{1 + O\left(\frac{\log\log t}{\log t}\right)^{\frac{1}{2}}\right\}.$$

The assumption (1) in the theorem of Copeland and Erdős as well as Corollary 2 is indispensable as the following theorem shows.

THEOREM. (Shiokawa [8]). *For any given* $\varepsilon > 0$, *there is an increasing sequence* $n_1, n_2, \ldots$ *of positive integers satisfying*

$$A(x) > x^{1-\varepsilon}$$

provided that x *is sufficiently large, such that* $\theta_r = 0.n_1 n_2 \ldots$ *is not normal to base* r.

The estimate obtained in Theorem 1 is best possible in the sense that $O((\log(x/A(x)) + \log\log x)/\log x)^{\frac{1}{2}}$ cannot be replaced by $o((\log(x/A(x)) + \log\log x)/\log x)^{\frac{1}{2}}$. The same is true for Theorem 2, and when $r = 2$ for Corollary 1, since $N_2(n;1) = s_2(n)$. Indeed we have the following

THEOREM 3. *Let* b *be one of* $0,1,\ldots,r-1$. *Then there is an increasing sequence* $n_1, n_2, \ldots$ *of positive integers satisfying*

$$A(x) > \frac{1}{r^2} \frac{x}{\log x}$$

for all sufficiently large x *such that*

$$\sum_{n_i \le x} N_r(n_i;b) \ge \left(1 + \frac{1}{120} \frac{r \log\log x}{\log x}\right)^{\frac{1}{2}} \frac{1}{r} A(x) \log_r x$$

for infinitely many integers x.

For some specified sequences $n_1, n_2, \ldots$ satisfying the condition (1), one may get better results than those which can be deduced from Theorem 1. For instance, we can show the following by a method similar to that used in [3]: Let l and m be integers such that $0 \le l < m$, and let $b_1, b_2, \ldots, b_l$ be as in Theorem 1. Then

$$\sum_{\substack{n \le x \\ n \equiv a \pmod m}} N_r(n; b_1 b_2 \ldots b_l) = \frac{1}{r^l} \frac{x}{m} \log_r x + O(x)$$

and

$$\sum_{\substack{n \le x \\ (n,m)=1}} N_r(n; b_1 b_2 \ldots b_l) = \frac{1}{r^l} \frac{\varphi(m)}{m} x \log_r x + O(d(m)x) .$$

where $d(n)$ is the number of divisors of n. By (1) we also have the estimates for the corresponding sums of digits as Corollary 1.

Finally we exhibit a theorem which is of interest in connection with Example 1.

THEOREM 4. *For any* l *integers* $b_1, b_2, \ldots, b_l$ *with* $0 \le b_i < r$, *we have*

$$\sum_{n \le x} \sum_{\substack{m \le n \\ (m,n)=1}} N_r(n; b_1 b_2 \ldots b_l)$$

$$= \left(1 + O\left(\frac{\log \log x}{\log x}\right)\right) \frac{1}{r^l} \frac{3}{\pi^2} x^2 \log_r x ,$$

as $x \to \infty$, *where the constant implied depends possibly on* r *and* 1. *Especially,*

$$\sum_{n\le x} \sum_{\substack{m\le n \\ (m,n)=1}} s_r(m) = \left(1+0\left(\frac{\log\log x}{\log x}\right)\right) \frac{r-1}{2}\frac{3}{\pi^2} x^2 \log_r x .$$

2. PROOFS

For the proofs of Theorems 1 and 3, we need the following Lemma which is a refinement of those proved in [7] and [8]. We denote by $T(k,\varepsilon;b)$ and $S(k,\varepsilon;b)$ the number of integers n with $0 \le n < r^k$ such that $|N_r(n;b) - k/r| > k\varepsilon$ and $N_r(n;b) - k/r > k\varepsilon$, respectively.

LEMMA. *Let* b *be any integer with* $0 \le b < r$. *Then we have*

$$T(k,\varepsilon;b) < r^k\, k \exp\left(-\frac{1}{32} k\varepsilon^2\right)$$

and

$$S(k,\varepsilon;b) > \frac{1}{r}\frac{r^k}{\sqrt{k}} \exp\left(-72rk\varepsilon^2\right)$$

for any ε *with* $0 < \varepsilon < 1/8$ *and any integer* k *with* $k\varepsilon \ge 4r$.

Proof of the first inequality. Putting $p(mr,1) = \left\{\begin{matrix} mr \\ 1 \end{matrix}\right\}(r-1)^{mr-1}$ for brevity, we have

$$T(mr,\varepsilon/2) \le \sum_{|1-m|>mr\varepsilon/2} p(mr,1)$$

$$= \sum_{|j|>mr\varepsilon/2} p(mr,m+j) < r^{mr} mr \exp(-\frac{1}{16} mr\varepsilon^2) ,$$

provided $mr\varepsilon \ge 2$, using the inequality (see [6]) $p(mr,m+j) < r^{mr} \exp(-j^2/(4mr))$, where j is an integer with $|j| \ge 2$. Now let $k = mr + d$, $0 \le d < r$. Then writing $n < r^k$ as (2) and putting $n_1 = \sum_{i=d+1}^{k} a_i r^{k-i}$, we have $|N(n) - k/r| < |N(n_1) - m| + r$, so that if $|N(n)-k/r| > k\varepsilon$, we have $|N(n_1) - m| > mr\varepsilon/2$, provided $k\varepsilon \ge 4r$. Therefore we obtain

$$T(k,\varepsilon;b) < r^d T(mr,\varepsilon/2) < r^k k \exp(-\frac{1}{32} k\varepsilon^2).$$

Proof of the second inequality. Assume first that $b \neq 0$. We write $k = mr + d$, $0 \le d < r$. Then

$$S(mr,2\varepsilon;b) = \sum_{1-m>2mr\varepsilon} p(mr,1) = \sum_{2mr\varepsilon<j\le mr-m} p(mr,m+j)$$

$$> p(mr,m+j_0), \; j_0 = [2mr\varepsilon]+1 \; .$$

Using the inequality $1 - x > e^{-2x}$ with $0 \le x \le 1/2$, we have

$$p(mr,m+j_0)/p(mr,m) = \prod_{i=1}^{j_0} (1 - \frac{i-1}{mr-m})/(1+\frac{i}{m}) >$$

$$> \exp(-\frac{2}{m} j_0^2) ,$$

noticing that $\varepsilon < 1/8$ implies $(j_0-1)/(mr-m) \le 1/2$. This together with the inequality

$$p(mr,m) > r^{mr}/\sqrt{m}$$

leads to

$$S(mr,2\varepsilon;b) > \frac{r^{mr}}{\sqrt{m}} \exp(-\frac{2}{m} j_0^2) > \frac{r^{mr}}{\sqrt{m}} \exp(-18mr^2\varepsilon^2)$$

provided $mr\varepsilon > 1$. Now let n_1 be as above. If $N_r(n_1;b)-m > 2mr\varepsilon$, we have $N_r(n;b)-k/r > N_r(n_1;b)-k/r > N_r(n_1;b)-m-1 > k\varepsilon$, provided $k\varepsilon \ge 4r$. Hence we obtain

$$S(k,\varepsilon;b) \ge r^d S(mr,2\varepsilon;b) > \frac{r^k}{\sqrt{k}} \exp(-18rk\varepsilon^2) .$$

For the remaining case of $b = 0$, we get

$$S(k,\varepsilon;0) \ge \sum_{\substack{(r-1)r^{k-1} \le n < r^k \\ N_r(n;0)-k/r > k\varepsilon}} 1 =$$

$$= \sum_{\substack{(r-1)r^{k-1} \le n < r^k \\ N_r(n;r-1)-1-k/r > k\varepsilon}} 1$$

$$\ge \sum_{\substack{(r-1)r^{k-1} \le n < r^k \\ N_r(n;r-1)-1-(k-1)/r > 2\varepsilon(k-1)}} 1$$

$$= S(k-1,2\varepsilon;r-1) \ge \frac{1}{r} \frac{r^k}{\sqrt{k}} \exp(-72rk\varepsilon^2),$$

as required, and the proof of Lemma is completed.

Proof of Theorem 1. Assume first that l=1. Putting $k = [\log_r x + 1]$, we have

$$\Big|\sum_{n_i \le x} N(n_i) - \frac{A(x)}{r}\log_r x\Big| \le \Big|\sum_{n_i \le x} N(n_i) - \frac{A(x)}{r}k\Big|$$

$$+ \Big|\frac{A(x)}{r}k - \frac{A(x)}{r}\log_r x\Big| \le$$

$$\le \Big(\sum_{\substack{n_i \le x \\ |N(n_i)-k/r| \le k\varepsilon}} + \sum_{\substack{n_i \le x \\ |N(n_i)-k/r| > k\varepsilon}}\Big)\Big|N(n_i) - \frac{k}{r}\Big|$$

$$+ \frac{A(x)}{r} \le A(x)k\varepsilon + \frac{A(x)}{r} + kT(k,\varepsilon;b),$$

where $\varepsilon = \varepsilon(x)$ is defined by

$$\varepsilon^2 = \frac{2^5}{k}\left(\log \frac{r^k}{A(x)} + 2\log k\right),$$

so that, by the assumption $x \ge r^{r^2}$, we find $k\varepsilon \ge 4r$ and

$$\varepsilon^2 < \frac{2^8}{\log_r x}\left(\log \frac{x}{A(x)} + \log(\log_r x)\right). \tag{5}$$

Thus we may use the first inequality of Lemma and obtain $T(k,\varepsilon;b) < A(x)/k$. Therefore

$$\Big|\sum_{n_i \le x} N(n_i) - r^{-1}A(x)\log_r x\Big| < A(x)k\varepsilon + A(x)/r + A(x)$$

$$< 4\varepsilon\, A(x)\log_r x\,,$$

which together with (5)

leads to

$$(6) \qquad \leq 2^6 \left(\frac{\log(x/A(x)) + \log(\log_r x)}{\log_r x} \right)^{\frac{1}{2}} A(x)\log_r x \,.$$

Now let $l \geq 2$. It follows from the definition that

$$|N_r(n;b_1b_2\ldots b_l) - \sum_{j=0}^{l-1} N_{r^l}([nr^{-i}];B)| \leq 1,$$

where $B = \sum_{i=1}^{l} b_i r^{l-1}$, so that

$$\Big| \sum_{n_i \leq x} N_{r^l}(n_i;b_1b_2\ldots b_l) - r^{-l}A(x)\log_r x \Big|$$

$$\leq \sum_{j=0}^{l-1} \Big| \sum_{n_i \leq x} N_{r^l}([n_i r^{-j}];B)$$

$$- r^{-l}A(x)\log_{r^l}(xr^{-j}) \Big| + 2lA(x),$$

and hence using (6) with r^l and xr^{-j} in place of r and x,

$$\leq 2^7 l \max_{y \leq x} \left(\frac{\log(y/A(y)) + \log(\log_{r^l} y)}{\log_{r^l} y} \right)^{\frac{1}{2}} A(y)\log_{r^l} y + 2lA(x),$$

provided $x \geq r^{lr^{2l}}$, which leads to Theorem 1.

Proof of Theorem 2. We put for brevity

$$N(t) = N(t;\theta_r;b_1b_2\ldots b_l),$$

$$N(m) = N_r(m;\, b_1b_2\ldots b_l),$$

$$K(m) = [\log_r m] + 1, \text{ and } n = n(t).$$

Then

$$t = \sum_{n_i \le n} K(n_i) + 0(\log n) \tag{7}$$

and

$$N(t) = \sum_{n_i \le n} N(n_i) + 0(\log n) + 0(A(n)),$$

so that

$$\frac{N(t)}{t} = \frac{\sum_{n_i \le n} N(n_i)}{\sum_{n_i \le n} K(n_i)} + 0\left(\frac{\log n}{t}\right), \tag{8}$$

noticing that $A(n) = 0(\log n)$ by (1).

Now putting $k = K(n)$, we get

$$A(n)k - \sum_{n_i \le n} K(n_i) = \sum_{j=1}^{k-1} A(r^j - 1), \tag{9}$$

and so

$$\frac{\sum_{n_i \le n} N(n_i)}{\sum_{n_i \le n} K(n_i)} = \frac{\sum_{n_i \le n} N(n_i)}{A(n)k} \left\{ 1 + \frac{\sum_{j=1}^{k-1} A(r^j - 1)}{\sum_{n_i \le n} K(n_i)} \right\}. \tag{10}$$

Here

$$\sum_{j=1}^{k-1} A(r^j) \le \sum_{1\le j\le [\log_r A(r^{k-1})]} r^j + (k-1-[\log_r A(r^{k-1})])\, A(r^{k-1})$$

$$\le (3 + \log_r \frac{r^{k-1}}{A(r^{k-1})})\, A(r^{k-1}),$$

so that by (1) and (9)

$$(11) \qquad \sum_{n_i \le n} K(n_i) = A(n)k(1 + 0(1)),$$

and consequently

$$\frac{\sum_{j=1}^{k-1} A(r^j-1)}{\sum_{n_i \le n} K(n_i)} = 0(\frac{1}{k}) + 0(\frac{A(r^{k-1})}{kA(n)} (\log \frac{n}{A(n)} + \log \frac{A(n)}{A(r^{k-1})} + \log \frac{r^{k-1}}{n}))$$

$$= 0(\frac{1}{\log n}) + 0(\frac{1}{\log n} \log \frac{n}{A(n)}) .$$

Therefore we obtain by (1) and Theorem 1

$$\frac{\sum_{n_i \le n} N(n_i)}{\sum_{n_i \le n} K(n_i)} = \frac{1}{r^1} + 0(\frac{\log \frac{n}{A(n)} + \log \log n}{\log n})^{\frac{1}{2}} ,$$

which togetner with (8) yealds Theorem 2, since by (7) and (11) $\log t = \log n + 0(\log n)$, and so

$\log(n/A(n)) = O(\log t)$.

Proof of Theorem 3. Let k_0 be a sufficiently large integer. We put

$$\varepsilon_k = \frac{1}{12}\left(\frac{\log k - 2\log r}{rk}\right)^{\frac{1}{2}},$$

so that

$$\frac{1}{r}\frac{r^k}{\sqrt{k}}\exp(-72rk\varepsilon_k^2) = \frac{r^k}{k},$$

and $0 < \varepsilon_k < 1/8$, $k\varepsilon_k \geq 4r$ for all $k \geq k_0$. Since

$$\sum_{\substack{r^{k-1}\leq n<r^k \\ N_r(n;b)-k/r>k\varepsilon_k}} 1 > \frac{1}{r}S(k,\varepsilon_k;b),$$

we can choose, by the second inequality of Lemma, $[(r^k/k]+1)/r$ integers n's such that $r^{k-1}\leq n<r^k$ and $N_r(n;b)-k/r>k\varepsilon_k$. We denote by $n_1, n_2, \ldots$ the increasing sequence consisting of all these integers for all $k \geq k_0$. Then we have

$$\frac{A(x)}{x} \geq \frac{A(r^{[\log_r x]})}{r^{[\log_r x]+1}} > \frac{1}{r^2\log_r x} \tag{12}$$

and

$$\sum_{n_i\leq r^k} N_r(n_i;b) - \frac{1}{r}A(r^k)k$$

$$(13) \qquad = \sum_{i=k_0}^{k} \sum_{r^{j-1} \le n_i < r^j} (N_r(n_i;b) - \frac{k}{r})$$

$$- \frac{1}{r^2} \sum_{j=k_0}^{k} (k-j)([\frac{k}{j}] + 1) > \varepsilon_k r^k - \frac{2}{r^2} \sum_{j=1}^{k} (k-j) \frac{r^j}{j} .$$

By the partial summation formula, we get

$$\sum_{j=1}^{k} \frac{r^j}{j} \le \frac{r^{k+1}-1}{(r-1)k} + \frac{5r^{k+1}}{(r-1)k^2} < \frac{4r^k}{k} ,$$

so that

$$(14) \qquad \sum_{j=1}^{k} (k-j) \frac{r^j}{j} < \frac{10r^k}{k}$$

and

$$(15) \qquad A(r^k) \le \frac{1}{r} \sum_{j=1}^{k} (\frac{r^j}{i} + 1) < \frac{5r^k}{k} .$$

Combining (12), (13), (14), and (15), we obtain

$$\sum_{n_i \le r^k} N_r(n_i;b) > (1 + \frac{\varepsilon_k r^{k+1}}{A(r^k)k} - \frac{20r^{k-1}}{A(r^k)k^2}) \frac{1}{r} A(r^k)k$$

$$> (1 + \frac{1}{120} (\frac{r \log k}{k})^{\frac{1}{2}}) \frac{1}{r} A(r^k)k$$

for all $k \ge k_0$; which as well as (12) implies that the sequence $n_1, n_2, \ldots$ satisfies the properties mentioned in the theorem.

Proof of Theorem 4. We note first that for any integer b with $0 \le b < r$

$$\sum_{n\le x} N_r(n;b) = \frac{x}{r}\log_r x + O(x) ,$$

(which can be proved for instance by the same idea as in [5],) and so

$$(15) \qquad \sum_{n\le x} N_r(n;b_1b_2\ldots b_1) = \frac{x}{r^1}\log_r x + O(x) .$$

Now we put

$$\lambda = [\log_r(\log n)] \text{ and } J = [nr^{-\lambda}]$$

so that $Jr^\lambda \le n < (J+1)r^\lambda$. We note that for any integer $j \ge 0$,

$$N(j) \le N(m) \le N(j) + \lambda$$

if m is an integer with $jr^\lambda \le m < (j+1)r^\lambda$, where $N(n) = N_r(n;b_1b_2\ldots b_1)$. Then, using the equality (see [6])

$$\sum_{\substack{m\le q\\(m,n)=1}} 1 = \frac{\varphi(n)}{n}q - \sum_{d\mid n}\mu(d)\{\frac{q}{d}\}$$

where n and q are positive integers and $\{x\} = x - [x]$, we get

$$\sum_{\substack{m\le n\\(m,n)=1}} N(m) = \sum_{j=1}^{j} \sum_{\substack{(j-1)r^\lambda<m\le jr^\lambda\\(m,n)=1}} N(m) + \sum_{Jr^\lambda<m\le n} N(m)$$

$$= \sum_{j=1}^{J} N(j) \sum_{\substack{(j-1)r^\lambda<m\le jr^\lambda\\(m,n)=1}} 1 + O(\lambda\varphi(n)) + O(r^\lambda \log n)$$

(16)

$$= \frac{\varphi(n)}{n} r^\lambda \sum_{j=1}^{J} N(j) - \sum_{j=1}^{J} N(j) \sum_{d|n} \mu(d)\left(\left\{\frac{jr^1}{d}\right\} - \left\{\frac{(j-1)r^1}{d}\right\}\right) +$$

$$+ O(\varphi(n) \log\log n) .$$

Here it follows from (15) that

(17) $$\frac{\varphi(n)}{n} r^\lambda \sum_{j=1}^{J} N(j) = \frac{\varphi(n)}{r^1} \log n + O(\varphi(n) \log\log n).$$

On the other hand, we have

$$\sum_{j=1}^{J} N(j) \sum_{d|n} \mu(d)\left(\left\{\frac{jr^1}{d}\right\} - \left\{\frac{(j-1)r^1}{d}\right\}\right) =$$

$$= N(J) \sum_{d|n} \mu(d)\left\{\frac{Jr^1}{d}\right\} - \sum_{j=2}^{J} (N(j) - N(j-1) \sum_{d|n} \mu(d)\left\{\frac{(j-1)r^1}{d}\right\}$$

(18)

$$= O(N(J)d(n)) + O(d(n) \sum_{j=1}^{J} |N(j) - N(j-1)|)$$

$$= O(d(n)n/\log n),$$

where $d(n)$ is the number of divisors of n, since

$$\sum_{j=1}^{J} |N(j) - N(j-1)| \le \sum_{k\ge 0} \sum_{J=1}^{J} \sum_{r^k \| j} (k+1) = O(J).$$

Combining (16), (17), and (18), we get

$$\sum_{\substack{m\le n \\ (m,n)=1}} N(m) = \frac{\varphi(n)}{r^1} \log_r n + O(\varphi(n)\log\log n) + O\left(\frac{d(n)n}{\log n}\right).$$

Therefore we obtain

$$\sum_{n\le x} \sum_{\substack{m\le n \\ (m,n)=1}} N(m) = \frac{1}{r^1} \sum_{n\le x} \varphi(n)\log_r n + O\Big(\sum_{n\le x} \varphi(n)\log\log n\Big) + O\Big(\sum_{n\le x} d(n)\,\frac{n}{\log n}\Big) =$$

$$= \frac{1}{r^1}\frac{3}{\pi^2} x^2 \log_r x + O(x^2 \log\log x),$$

using the inequalities

$$\sum_{n\le x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \log x)$$

and

$$\sum_{n\le x} d(n) = x \log x + O(x),$$

and the proof of Theorem 4 is completed.

REFERENCES

[1] COPELAND, A.H. and ERDŐS, P., Note on normal numbers. *Bull. Amer. Math. Soc.*, 52, (1946), 857-860.

[2] HEPPNER, E., Über die Summe der Ziffern natürlicher Zahlen. Ann. Univ. Sci. Budapest, Rolando Eötvös nom. Sect. Math., 19 (1967), 41-43.

[3] KÁTAI, I., On the sum of digits of prime numbers. Ann. Univ. Sci. Budapest, Rolando Eötvös nom. Sect. Math., 10 (1967), 89-93.

[4] KÁTAI, I., On the sum of digits of primes. *Acta Math. Acad. Sci. Hungaricae*, 30 (1977), 169-173.

[5] MIRSKY, L., A theorem on representations of integers in the scale of r. Scripta Math., 15 (1946), 11-12.

[6] NIEDERREITER, H., The distribution of Farey points. *Math. Ann.* 201 (1973), 341-345.

[7] NIVEN, I., Irrational Numbers. The Carus Math. Monogr. No. 11, Math. Assoc. Amer., Washington, D.C., 1956, Chap. 8.

[8] SHIOKAWA, I., A remark on a theorem of Copeland-Erdős. Proc. Japan Acad., 50 (1974), 273-276.

[9] SHIOKAWA, I., On the sum of digits of prime numbers.
Proc. Japan Acad., 50 (1974), 551-554.

IEKATA SHIOKAWA
Department of Mathematics
Keio University
Hiyoshi, Kohokuku, Yokohama
223 Japan

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ASYMPTOTIC DISTRIBUTION OF PARTITIONS BY NUMBER AND SIZE OF PARTS

SZEKERES, G.

Let $p(n;k)$ denote the number of partitions of n in exactly k positive integer parts (or what is the same, into parts with largest summand k), $p(n;r,k)$ the number of partitions of n in r parts and maximal summand k, $q(n;r,k)$ the number of partitions of n in r unequal parts and largest summand k. In a recent paper [4] I have determined the asymptotic distribution of $q(n;r,k)$ for large n when r was in a suitable neighbourhood of $\frac{2\sqrt{3}\ \log 2}{\pi}\sqrt{n}$ and k in a suitable neighbourhood of $\frac{2\sqrt{3}}{\pi}\, n\sqrt{\log n}$ (the places where the r- and k-distributions reach their respective asymptotic maxima). The corresponding problem for $p(n;r,k)$ was left open. In this note we consider this second problem.

First, a few remarks concerning $p(n;k)$. According to an old result of Erdős and Lehner [2], for almost all partitions the maximal summand

$$k = \frac{\sqrt{n}}{c} \log\sqrt{n} + O(\sqrt{n}\omega(n)) \text{ where } c = \pi/\sqrt{6} = 1.28254983...$$

and $\omega(n)$ is any positive function which increases to infinity arbitrarily slowly. For fixed large n, $p(n;k)$ has a so-called doubly exponential (or extreme value) distribution in the neighbourhood of the median $k_o = \frac{\sqrt{n}}{c} \log \frac{\sqrt{n}}{c}$. More specifically if $y = \frac{c}{\sqrt{n}} (k-k_o)$ and say $|k-k_o| < \frac{1}{4c}\sqrt{n}\log\sqrt{n}$ then

$$p(n;k) \sim P(n) \frac{c}{\sqrt{n}} \exp(-y-e^{-y}) \tag{1}$$

where

$$P(n) \sim \frac{1}{4\sqrt{3n}} \exp(2c\sqrt{n})$$

is the total number of partitions of n. The symbol $\sim$ means that the quotient of the two sides tends to 1 when $n\to\infty$. The distribution (1) can be obtained without much difficulty from the main asymptotic formula in [3], but will also follow directly from Theorem 1 below.

For fixed r in the neighbourhood of $r_o = k_o$ we expect $p(n;r,k)$ to have the same distribution as $p(n;k)$ itself (in some neighbourhood of k_o), with $P(n)$ replaced by $p(n;r)$ in (1). Of course once we are sufficiently away from the peak k_o, correlations will set in between

the r- and k-distributions and we shall examine the be-behaviour of $p(n;r,k)$ over a sufficiently large range of r and k to exhibit the form of these correlations. Specifically we assume that

$$(2) \qquad \frac{1}{4}\frac{\sqrt{n}}{c}\log n < r,k < \frac{1}{c}n^{3/4}/\log n.$$

We set

$$(3) \qquad \lambda = \frac{ck}{\sqrt{n}}\ ,\ \mu = \frac{cr}{\sqrt{n}}$$

so that

$$(4) \qquad \frac{1}{4}\log n < \lambda,\mu < n^{1/4}/\log n.$$

We also set

$$L(x) = \int_x^\infty \frac{t}{e^t - 1}\,dt \qquad \text{for } x \geq 0$$

so that

$$(5) \qquad L(0) = c^2$$

and $L(x) = \int_x^\infty te^{-t}\,dt + \int_x^\infty te^{-2t}\,dt + O\left(\int_x^\infty te^{-3t}\,dt\right)$, hence

$$(6) \quad L(x) = (1+x)e^{-x} + \frac{1}{4}(1+2x)\,e^{-2x} + O(xe^{-3x}) \text{ when } x \to \infty\ .$$

THEOREM 1. Suppose $\lambda = \frac{ck}{\sqrt{n}}$, $\mu = \frac{cr}{\sqrt{n}}$ satisfy the inequalities

$$\frac{1}{4}\log n < \lambda,\mu < n^{\frac{1}{4}}/\log n.$$

$$(7)\quad p(n;r,k)\sim P(n).\exp\{-(\lambda+\mu)-\frac{\sqrt{n}}{c}(e^{-\lambda}+e^{-\mu})-\frac{\sqrt{n}}{4c}(e^{-2\lambda}+e^{-2\mu})$$

$$-\frac{\sqrt{n}}{4c^3}((\lambda+1)^2\,e^{-2\lambda}+(\mu+1)^2\,e^{-2\mu})+\frac{\sqrt{n}}{e}e^{-(\lambda+\mu)}$$

$$-\frac{\sqrt{n}}{2c^3}(\lambda+1)(\mu+1)\,e^{-(\lambda+\mu)}+\frac{1}{2c^2}\lambda\mu\,(e^{-\lambda}+e^{-\mu})\}$$

where $P(n)\sim\frac{1}{4\sqrt{3}n}\exp(2c\sqrt{n})$ is the total number of unrestricted partitions of n.

Formula (7) is of course symmetric in λ and μ, in accordance with the symmetry of $p(n;r,k)$ with respect to r and k, due to the interchange of the roles of the number of parts and maximal summand in a pair of conjugate partitions.

If $\frac{\sqrt{n}}{c}\log n > r,k > \frac{\sqrt{n}}{c}(\frac{1}{4}+\epsilon)\log n$ for some $\epsilon>0$ then all correlation terms disappear and we have

COROLLARY. If $(\frac{1}{4}+\epsilon)\log n<\lambda,\ \log n$ for some $\epsilon>0$ then

$$(8)\quad p(n;r,k)\sim P(n).\exp\{-(\lambda+\mu)-\sqrt{\frac{n}{c}}(e^{-\lambda}+e^{-\mu})\}.$$

Hence in this neighbourhood of k_o the r- and k-distributions are doubly exponential (extreme value) and independent. The range of k and r in which the distributions are independent is sufficiently wide to cover

almost all partitions. This follows immediately from Erdős and Lehner [2], but can also be seen from

$$\int_{(\frac{1}{4}\sqrt{n}/c)\log n}^{(\sqrt{n}/c)\log n} \exp\{-\lambda - \frac{n}{c}e^{-\lambda}\}dk = \frac{\sqrt{n}}{c}\int_{\frac{1}{4}\log n}^{\log n} \exp\{-\lambda - \frac{\sqrt{n}}{c}e^{-\lambda}\}d\lambda$$

$$= \int_{n^{-\frac{1}{2}}/c}^{n^{\frac{1}{4}}/c} e^{-t}dt \sim 1.$$

From here it follows

THEOREM 2. If $(\frac{1}{4}+\varepsilon)\log n < \lambda < \log n$ then

$$p(n;k) \sim P(n).\exp\{-\lambda - \frac{\sqrt{n}}{c}e^{-\lambda}\}.$$

In particular if $\frac{1}{2}\log n - \omega(n) < \lambda < \frac{1}{2}\log n + \omega(n)$ where $\omega(n)$ grows to ∞ arbitrarily slowly then

$$\frac{\sqrt{n}}{c}\int_{\frac{3}{2}\log n - \omega(n)}^{\frac{1}{2}\log n + \omega(n)} \exp\{-\lambda - \frac{\sqrt{n}}{c}e^{-\lambda}\}d\lambda = \int_{\frac{1}{c}e^{-\omega(n)}}^{\frac{1}{c}e^{\omega(n)}} e^{-t}dt \sim 1,$$

and we obtain the theorem of Erdős and Lehner: in almost all partitions the number of terms (or maximal summand) is $\frac{\sqrt{n}}{c}\{\log\sqrt{n} + O(\omega(n))\}$.

To prove Theorem 1 we start from the standard

generating function (see Andrews [1], p33)

$$q^{r+k-1}\,\frac{(1-q^r)\ldots(1-q^{r+k-2})}{(1-q)\ \ldots(1-q^{k-1})} = \sum_{n=0}^{\infty} p(n;r,k)q^n$$

which seems more convenient for the present problem than the 2-parameter generating function used in [4]. By Cauchy

$$(9)\quad p(n;r,k) = \frac{1}{2\pi i}\int z^{r+k-n-2}\exp\{-\sum_{\nu=1}^{k-1}\log(1-z^\nu) + \sum_{\nu=r}^{k+r-2}\log(1-z^\nu)\}dz$$

taken over $z = e^{-\beta+i\theta}$, $-\pi<\theta\leqq\pi$ for some $\beta>0$. We determine β from the saddle point condition

$$(10)\quad \sum_{\nu=1}^{k-1}\frac{\nu}{e^{\beta\nu}-1} - \sum_{\nu=r}^{k+r-2}\frac{\nu}{e^{\beta\nu}-1} = n - r - k\ .$$

From here it follows, since $ke^{-ck/\sqrt{n}} = o(\sqrt{n})$ by (2), that

$$(11)\quad n \sim \beta^{-2}\int_0^\infty \frac{t}{e^t-1}\,dt = c^2/\beta^2,$$

$$\beta \sim c/\sqrt{n}.$$

More precisely, by Euler-Maclaurin,

$$\sum_{\nu=1}^{k-1} \frac{\nu}{e^{\nu\beta}-1} = \frac{1}{\beta^2} \int_0^{\beta k} \frac{t}{e^t-1}\,dt - \frac{1}{2}\,\frac{k}{e^{k\beta}-1} - \frac{1}{2\beta} + \frac{1}{24} + o(1)$$

$$= \frac{1}{\beta^2}(c^2 - L(\beta k)) - \frac{1}{2\beta} + o(\sqrt{n}),$$

$$\sum_{\nu=r}^{r+k-2} \frac{\nu}{e^{\nu\beta}-1} = \frac{1}{\beta^2}\,(L(\beta r) - L(\beta(r+k))) + o(\sqrt{n})$$

and so the saddle point condition (10) gives

$$(12)\quad \frac{c^2}{\beta^2} - \frac{1}{\beta^2}\,(L(\beta r)+L(\beta k)-L(\beta(r+k))) = n-r-k+\frac{1}{2\beta}+o(\sqrt{n}),$$

$$\frac{1}{\beta^2} = \frac{n}{c^2}\left(1-\frac{r+k}{n}+\frac{1}{2\beta n}\right)\left\{1-\frac{1}{c^2}(L(\beta k)+L(\beta r))+\frac{1}{c^2}L(\beta(r+k))\right\}^{-1}+o(\sqrt{n}).$$

Taking conditions (2),(6) and (11) into account,

$$L(\beta k)=0(n^{-\frac{1}{4}+\delta}),\quad L(\beta r)=0(n^{-\frac{1}{4}+\delta}),\quad L(\beta(r+k))=0(n^{-\frac{1}{2}+\delta})$$

for arbitrarily small (fixed) $\delta>0$, hence by (2) and (3)

$$(13)\quad \frac{1}{\beta} = \frac{\sqrt{n}}{c} - \frac{1}{2c^2}(\lambda+\mu) + \frac{1}{4c^2} + \frac{\sqrt{n}}{2c^3}(L(\beta r)+L(\beta k)) - \frac{\sqrt{n}}{2c^3}L(\beta(r+k))$$

$$+ \frac{3}{8}\,\frac{\sqrt{n}}{c^5}(L(\beta r)+L(\beta k))^2 - \frac{1}{4c^4}(\lambda+\mu)\,(L(\beta r)+L(\beta k)) + o(1)$$

and

$$(14)\quad \beta = \frac{c}{\sqrt{n}} - \frac{1}{2c\sqrt{n}}(L(\beta r)+L(\beta k)) + \frac{\lambda+\mu}{2n} + O(n^{-1}\log^2 n).$$

Going back to (9),

$$(15)\quad p(n;r,k) \sim \frac{1}{2\pi} e^{\beta(n-r-k)} \int_{-n^{-5/7}}^{n^{-5/7}} \exp\{i\theta(r+k-n-1) -$$

$$- \sum_{\nu=1}^{k-1} \log(1-e^{-\beta\nu+i\nu\theta}) + \sum_{\nu=r}^{r+k-2} \log(1-e^{-\beta\nu+i\nu\theta})\}d\theta$$

(The complementary integrals over the rest of $(-\pi,\pi)$ are negligible, by standard arguments). Here

$$-\sum_{\nu=1}^{k-1} \log(1-e^{-\nu\beta+i\nu\theta}) = -\sum_{\nu=1}^{k-1} \log(1-e^{-\beta\nu}) - \sum_{\nu=1}^{k-1} \log\left(1-\frac{\nu}{e^{\beta\nu}-1}i\theta+\right.$$

$$\left.+\frac{1}{2}\frac{\nu^2}{e^{\beta\nu}-1}\theta^2+\ldots\right) = -\sum_{\nu=1}^{k-1} \log(1-e^{-\beta\nu}) + \sum_{\nu=1}^{k-1} \frac{i\nu\theta}{e^{\beta\nu}-1} -$$

$$- \frac{1}{2}\sum_{\nu=1}^{k-1} \frac{\nu^2 e^{\beta\nu}}{(e^{\beta\nu}-1)^2}\theta^2 + O(n^{-1/7})$$

and similarly for $\sum_{\nu=r}^{k+r-2}$. The $i\theta$ terms in (15) cancel because of the saddle point condition, hence

$$p(n;r,k) \sim \frac{1}{2\pi} \exp\{\beta(n-r-k) - \sum_{\nu=1}^{k-1} \log(1-e^{-\nu\beta}) +$$

$$+ \sum_{\nu=r}^{k+r-2} \log(1-e^{-\nu\beta})\}.$$

$$\int_{-\infty}^{\infty} \exp\{-\frac{1}{2}\sum_{\nu=1}^{k-1}\frac{\nu^2 e^{\beta\nu}}{(e^{\beta\nu}-1)^2}\theta^2+\frac{1}{2}\sum_{\nu=r}^{k+r-2}\frac{\nu^2 e^{\beta\nu}}{(e^{\beta\nu}-1)^2}\theta^2\}d\theta.$$

The expression in the exponent of the integrand is

$$\sim -\frac{\theta^2}{2\beta^3}\int_0^{\infty}\frac{t^2e^t}{(e^t-1)^2}\,dt = -\frac{1}{c}n^{3/2}\theta^2 = -\frac{1}{\pi}6^{1/2}n^{3/2}\theta^2$$

by (11), hence

$$p(n;r,k)\sim\frac{1}{2.6^{1/4}n^{3/4}}\exp\{\beta(n-r-k)-\sum_{\nu=1}^{k-1}\log(1-e^{-\nu\beta})+ \tag{16}$$

$$+\sum_{\nu=r}^{r+k-2}\log(1-e^{-\nu\beta})\}.$$

It remains to evaluate the expression in the exponent of (16). Now

$$\beta(n-r-k)=\frac{c^2}{\beta}-\frac{1}{\beta}\left(L(\beta k)+L(\beta r)+\frac{1}{\beta}L(\beta(k+r))-\frac{1}{2}+o(1)\right.$$

by (12),

$$-\sum_{\nu=1}^{k-1}\log(1-e^{-\nu\beta})=\frac{c^2}{\beta}-\frac{1}{\beta}L(\beta k)-k\log(1-e^{-\beta k})+\frac{1}{2}\log\frac{\beta}{2\pi}+o(1)$$

(see [3], p 105, it follows easily from Euler-Maclaurin and Stirling's formula),

$$\sum_{\nu=r}^{r+k-2}\log(1-e^{-\nu\beta})=\frac{1}{\beta}\int_{\beta r}^{\beta(r+k)}\log(1-e^{-t})\,dt+o(1)$$

$$=-\frac{1}{\beta}L(\beta r)+\frac{1}{\beta}L(\beta(k+r))+(r+k)\log(1-e^{-\beta(r+k)})$$

$$-r\log(1-e^{-r\beta})+o(1).$$

Hence the expression in the exponent of (16) is

$$(17)\quad \frac{2c^2}{\beta} - \frac{2}{\beta}(L(\beta k)+L(\beta r))+\frac{2}{\beta}L(\beta(k+r))-k\log(1-e^{-k\beta})$$

$$-r\log(1-e^{-r\beta})+(k+r)\log(1-e^{-(k+r)\beta})-$$

$$-\frac{1}{2}+\frac{1}{2}\log\frac{\beta}{2\pi}+o(1).$$

Now from (3), (6) and (14)

$$k\beta = \lambda-\frac{1}{2c^2}\lambda((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})+\frac{\lambda}{2c\sqrt{n}}(\lambda+\mu)+0(\lambda n^{-1/2}\log^3 n),$$

$$e^{-k\beta}=e^{-\lambda}+\frac{1}{2c^2}\lambda e^{-\lambda}((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})-\frac{\lambda e^{-\lambda}}{2c\sqrt{n}}+0(\lambda^2 e^{-\lambda}n^{-1/2}\log^2 n)$$

$$L(\beta k)=(\lambda+1)e^{-\lambda}+\frac{1}{2c^2}\lambda^2 e^{-\lambda}((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})+\frac{1+2\lambda}{4}e^{-2\lambda}-$$

$$-\frac{\lambda^2 e^{-\lambda}}{2c\sqrt{n}}\mu+o\left(n^{-\frac{1}{2}}\right),$$

$$L(\beta k)+L(\beta r)=((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})\left(1+\frac{1}{2c^2}(\lambda^2 e^{-\lambda}+\mu^2 e^{-\mu})\right)-$$

$$-\frac{\lambda\mu}{2c\sqrt{n}}(\lambda e^{-\lambda}+\mu e^{-\mu})+\frac{1}{4}(e^{-2\lambda}+e^{-2\mu})+\frac{1}{2}(\lambda e^{-2\lambda}+\mu e^{-2\mu})+o(n^{-1/2})$$

$$L(\beta(k+r))=(\lambda+\mu+1)e^{-(\lambda+\mu)}+o(n^{-1/2}).$$

Substituting these and $1/\beta$ from (13) into (17) we obtain for the expression in the exponent of (16)

$$2c\sqrt{n} - (\lambda+\mu) - \frac{\sqrt{n}}{c}(e^{-\lambda}+e^{-\mu}) - \frac{\sqrt{n}}{4c}(e^{-2\lambda}+e^{-2\mu}) + \frac{\sqrt{n}}{c}e^{-(\lambda+\mu)}$$

$$-\frac{1}{4}\frac{\sqrt{n}}{c^3}((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})^2+\frac{1}{2c^2}(\lambda+\mu)((\lambda+1)e^{-\lambda}+(\mu+1)e^{-\mu})$$

$$+\frac{1}{2}\log\frac{\beta}{2\pi}+o(1).$$

From here and (16)

$$p(n;r,k)\sim\frac{1}{4\sqrt{3}\,n}e^{2c\sqrt{n}}\cdot\exp\{-(\lambda+\mu)-\frac{\sqrt{n}}{c}(e^{-\lambda}+e^{-\mu})-\frac{\sqrt{n}}{4c}(e^{-2\lambda}+e^{-2\mu})$$

$$-\frac{\sqrt{n}}{4c^3}((\lambda+1)^2e^{-2\lambda}+(\mu+1)^2e^{-2\mu})-\frac{\sqrt{n}}{2c^3}(\lambda+1)(\mu+1)e^{-(\lambda+\mu)}$$

$$+\frac{\sqrt{n}}{c}e^{-(\lambda+\mu)}+\frac{1}{2c^2}\lambda\mu(e^{-\lambda}+e^{-\mu})\},$$

as required.

The terms $-\frac{\sqrt{n}}{2c^3}(\lambda+1)(\mu+1)e^{-(\lambda+\mu)}+\frac{\sqrt{n}}{c}e^{-(\lambda+\mu)}$ exhibit the correlation of the r- and k-distributions when both λ and μ are about $\frac{1}{4}\log n$, and the term $\frac{1}{2c^2}\lambda\mu(e^{-\lambda}+e^{-\mu})$ when one of λ or μ is about $n^{\frac{1}{4}}/\log n$ and the other is about $\frac{1}{4}\log n$.

REFERENCES

[1] GEORGE E. Andrews, *The theory of partitions* (Addison-Wesley Publishing Co., 1976)

[2] P. ERDŐS and J. LEHNER, "The distribution of the number of summands in the partitions of a positive integer", *Duke Math. J.* 8(1941) 335-345

[3] G. SZEKERES, "Some asymptotic formulae in the theory of partitions (II)", *Quart. J. Math. Oxford* (2) 4 (1953) 96-111

[4] G. SZEKERES, "Asymptotic distribution of the number and size of parts in unequal partitions", *Bull. Australian Math. Soc.* 36(1987), 89-97.

SZEKERES, G.
University of New South Wales

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE SUMMATION OF MULTIPLICATIVE ARITHMETICAL FUNCTIONS

TULYAGANOV S.T.

BASIC NOTATIONS

k, l, m, n, r	denote natural numbers; p is a prime.
c	is the Euler-Mascheroni constant.
Γ	is the gamma-function.
f, g, h	are multiplicative functions.

$$\Pi_f(y,x) = \prod_{y<p\le x} \left(1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r} \right);$$

$$S_f(y,x) = \sum_{y<p\le x} \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r} \ln p^r.$$

$f*g$ is the arithmetical convolution of the functions f and g, that is

$$f*g(n) = \sum_{km=n} f(k)g(m).$$

$n|\pi_y$ means that all prime divisors of n are less than or equal to y (possibly $n = 1$).

$(n,\pi_y) = 1$ means that all prime divisors of n are greater than y (possibly $n = 1$).

n_y is the product of the prime divisors of n up to y (with the proper multiplicity).

1. INTRODUCTION

One of the directions in the study of summation of multiplicative functions aims at finding asymptotical formulas like

$$(1.1)\quad \sum_{n\le x} f(n) = C\frac{x}{\ln x}\Pi_f(1,x) + O\left(\frac{x}{\ln x}\Pi_{|f|}(1,x)\right)$$

and its various modifications and generalizations with possibly weak restrictions on the values of f at prime numbers. This problem was treated by many authors ([1], [5]-[9], [11], [15], [16]). They proposed various methods. The analytic method developed by G. Halász [1] led to a

considerable advance in this field.

In general, for the study of $\sum_{n\le x} f(n)$ the values of $f(p^r)$ for $r \ge 2$ do not play an important role, it is sufficient to assume that they do not grow too fast. Under the condition

$$(1.2) \qquad \sum_{p\le x} f(p) = (\tau_f + o(1)) \frac{x}{\ln x}$$

and some restrictions on $f(p^r)$, $r \ge 2$, the formula (1.1) was established by E. Wirsing [15] for nonnegative functions. B.V. Levin and A.S. Fainleib [7] proved (1.1) under the assumption (1.2) for multiplicative functions of the class W, defined by the conditions

$$\sum_{p\le x} |f(p)| = O(\frac{x}{\ln x})$$

and

$$f(p^r) = ((2p)^{\gamma r}) \quad \text{for} \quad r \ge 2, \quad \text{with} \quad 0 < \gamma < 1/2.$$

It is known that under the condition

$$(1.3) \qquad \sum_{p\le x} \frac{f(p)\ln p}{p} = (\tau_f + o(1))\ln x,$$

which is weaker than (1.2), (1.1) does not hold in general (see [9]). On the other hand, (1.1) follows from

(1.3) under some additional conditions. For instance, E. Wirsing [16] proved (1.1) for multiplicative functions that are bounded at the primes, satisfy (1.3) with a real $\tau_f > 0$ and

$$\sum_{p^r, r\geq 2} \frac{|f(p^r)|}{p^r} < \infty, \qquad \sum_{p} \frac{|f(p)|-\mathrm{Re}\, f(p)}{p} < \infty$$

(and $\sum_{p^r\leq x,\ r\geq 2} |f(p^r)| = O(x/\ln x)$, if $\tau_f \leq 1$).

B.V. Levin and A.S. Fainleib proved the following

THEOREM [9]: *Let* $f, h \in W$ *and assume that* f *satisfies* (1.3). *Then, if there exists a sequence* $g(p)$ *such that*

$$\sum_{p\leq x} |g(p)| = O\left(\frac{x}{\ln x}\right), \qquad \sum_{p\leq x} g(p)\ln p = (\tau_g + o(1))x$$

and

$$\sum_{y<p\leq x} \frac{|f(p)| - |f(p) - g(p)|}{p} \to +\infty$$

(1.4)

where $y = y(x)\to\infty$ as $x\to\infty$ but $(\ln x)/(\ln y) \to \infty$, *then there exists another* $y = y^*(x)$, $(\ln x)/(\ln y) \to \infty$

such that

$$(1.5)\quad \sum_{n\le x} h(n_y)f(n|n_y) = \frac{e^{-c\tau_f}}{\Gamma(\tau_f)}\frac{x}{\ln x}\Pi_h(1,y)\Pi_f(y,x) +$$

$$+ o\Big(\frac{x}{\ln x}\Pi_{|h|}(1,y)\Pi_{|f|}(y,x)\Big).$$

This result has lots of applications. In particular, from (1.3), with some additional assumptions on $f(p)$, the estimate (1.1) can be obtained [9].

Another direction in the theory of summation of multiplicative functions is to find asymptotic formulas like (1.1) with an estimation of the remainder term. B.V. Levin and A.S. Fainleib [8] found an asymptotical series for $\sum_{n\le x} f(n)$. The following results is due to J.P. Kubilius [3].

THEOREM. *Let* $f(n)$ *be a complex-valued multiplicative function. Assume that there exists a quantity* λ, *independent of* p, $|\lambda| \le c_1$, *such that*

$$\sum_p |f(p)-\lambda|\frac{\ln p}{p} < c_2, \qquad \sum_p \sum_{r=2}^{\infty} |f(p^r)|\frac{\ln p^r}{p^r} < c_3.$$

Then for $x \ge 20$ *we have*

$$\sum_{n\le x} f(n) = \frac{x(\ln x)^{\lambda-1}}{\Gamma(\lambda)} \prod_p (1-\frac{1}{p})^{\lambda} (1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r}) + BRx(\ln x)^{\lambda/2-1},$$

where

$$R = \begin{cases} (1-|\lambda|)^{-1/2} & |\lambda| < 1 - (\ln\ln x)^{-1}, \\ (\ln\ln x)^{1/2} & \text{for } \big||\lambda| - 1\big| \le (\ln\ln x)^{-1}, \\ (|\lambda|-1)^{-1/2} (\ln x)^{\frac{|\lambda|}{2}-\frac{1}{2}} & |\lambda| > 1+(\ln\ln x)^{-1}. \end{cases}$$

The infinite product is absolutely convergent. The quantity B *is bounded by a constant, depending only on* c_1, c_2, c_3.

This result had numerous applications in probabilistic number theory. The investigations of J.P. Kubilius were continued by E. Manstavious [10], A. Laurincikas [4], Z. Kryzius [2], S.T. Tulyaganov [14] and others.

In this paper we establish an asymptotical relation (Theorem 1), which, in particular, implies (1.5) for a nonempty class of multiplicative functions not satisfying (1.4). It will also allow us to make the "o" explicite. From the same result we shall deduce an asymptotical formula with a remainder term for the mean values of multiplicative functions (Theorem 3).

2. MAIN RESULTS

We call a multiplicative function f *exponentially multiplicative*, if for every prime p and natural number r it satisfies $f(p^r) = (f(p))^r/r!$.

By L we denote the class of multiplicative arithmetical functions that satisfy

$$\sum_{p^r \le x} |f(p^r)| \ln p^r \ll x$$

and

$$\sum_{r=1}^{\infty} r|f(p^r)|/p^r < \infty$$

for every p.

The main result of this paper is the following.

THEOREM 1. *Let* $f, g, h \in L$, *and let* g *be an exponentially multiplicative function satisfying*

$$\sum_{p \le x} g(p) \ln p = \tau x + O(x\rho(x)), \tag{2.1}$$

where $\tau \in C$, $|\tau| \le c_4$, $c_4 = constant$, $\rho(x) \downarrow 0$. *Then for every* $y = y(x)$ *satisfying* $\ln y = o(\ln x)$ *we have*

$$(1.2)\quad \sum_{n\le x} h(n_y)(f*g)(n/n_y) = \frac{e^{-C\tau}}{\Gamma(\tau)}\frac{x}{\ln x}\left(\frac{\ln x}{\ln y}\right)^{\tau} \Pi_h(1,y)\Pi_f(y,x) +$$

$$+ O\left(\frac{x}{\ln x}\Pi_{|h|}(1,y)\Pi_{|f|}(y,x)\left(\rho(y)\left(\frac{\ln x}{\ln y}\right)^{A}\ln\frac{\ln x}{\ln y} +\right.\right.$$

$$\left.\left. + \left(\frac{\ln x}{\ln y}\right)^{\max(0,\mathrm{Re}\,\tau-1)}\left(1+\frac{1}{\ln y}\left(S_{|h|}(1,y)+S_{|f|}(y,x,)\right)\right)\right)\right),$$

where A *is any number satisfying the condition*

$$\sum_{t<p\le z}\frac{|g(p)|}{p} \le A\ln\frac{\ln z}{\ln t} + O(1).$$

The existence of such a number A *follows from* $g\in L$.

We state some corollaries of Theorem 1.

THEOREM 2: *Let* f, h *be multiplicative functions bounded by one in the modulus,* g(p) *a sequences satisfying* (2.1) *and* $|g(p)| \le 1$. *Then for every* $y = y(x)$ *such that* $\ln y = o(\ln x)$ *and*

$$\int_y^x \rho(u)\, d\ln\ln u = O(1)$$

we have, with the same A *as in Theorem* 1,

$$\sum_{n\le x} h(n_y)\, f(n/n_y) = \frac{e^{-c\tau}}{\Gamma(\tau)}\,\frac{x}{\ln x}\,\Pi_h(1,y)\,\Pi_f(y,x) +$$

$$+ O\Big(\frac{x}{\ln x}\Big(\rho(y)\Big(\frac{\ln x}{\ln y}\Big)^{A} \ln\frac{\ln x}{\ln y} + 1 + \frac{1}{\ln y}\sum_{y<p\le x}\frac{|f(p)-g(p)|}{p}\ln p\Big)\times$$

$$\times \exp\Big(\sum_{p\le y}\frac{|h(p)|}{p} + \sum_{y<p\le x}\frac{|f(p)-g(p)|}{p}\Big)\Big).$$

Suppose that the multiplicative function f,h and the sequence $g(p)$ satisfies the conditions of Theorem 2 and

$$\sum_{p\le x}\frac{|f(p)|}{p} = \frac{\ln\ln x}{\ln\ln\ln x} + O(1), \quad \sum_{p\le x}\frac{|f(p)-g(p)|}{p}\ln p = O(\sqrt{\ln x}).$$

Then we have $\tau = 0$ and it is easy to see that the condition (1.4) does not hold for any choice of $g(p)$. Still, in this case from Theorem 2 we can deduce the existence of $y = y(x)$ such that

$$\sum_{n\le x} h(n_y) f(n/n_y) = O\Big(\frac{x}{\ln x}\exp\sum_{p\le y}\frac{|h(p)|}{p}\Big) = o(x).$$

If $\rho(x)$ is known, it is possible to determine $y = y(x)$

and specify the "o" in the remainder. For example, in case $\rho(x) = \exp(-a\sqrt{\ln x})$ from Theorem 2 with $y = \exp\sqrt{\ln x}$ we obtain

$$\sum_{n\le x} h(n_y) f(n/n_y) = \left(\frac{x}{\sqrt{\ln x}}\right).$$

The next result also follows from Theorem 1.

THEOREM 3. *Assume* $f,\ h\in L$,

$$\sum_p \sum_{r=2}^{\infty} \frac{|f(p^r)|}{p^r} < \infty, \quad \sum_p \frac{|f(p)|^2}{p^2} \ln p < \infty$$

and let the sequence $g(p)$ *satisfy* (2.1) *and*

$$\sum_p \frac{|g(p)|^2}{p^2} \ln p < \infty, \quad \sum_{p\le x} |g(p)| \ln p \ll x.$$

Then with every $y = y(x) \to \infty$ *such that* $\ln y = o(\ln x)$ *and*

$$\int_y^x \rho(u)\, d \ln\ln u = O(1)$$

the following asymptotical estimate holds:

$$(2.3)\quad \sum_{n\le x} h(n_y) f(n/n_y) = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{x}{\ln x} \Pi_h(1,y)\Pi_f(y,x) +$$

$$+ O\Big(\frac{x}{\ln x}\Pi_{|h|}(1,y)\Big((y)\Big(\frac{\ln x}{\ln y}\Big)^{A} \ln\frac{\ln x}{\ln y} + \Big(\frac{\ln x}{\ln y}\Big)^{\max(0,\mathrm{Re}\,-1)} (1 +$$

$$+ \frac{1}{\ln y}\Big(\sum_{p\le y}\sum_{r=1} \frac{|h(p^r)|}{p^r} \ln p^r + \sum_{y<p\le x} \frac{|f(p)-g(p)|}{p} \ln p +$$

$$+ \sum_{y<p\le x}\sum_{r=2}^{\infty} \frac{|f(p^r)|}{p^r} \ln p^r\Big)\Big) \exp \sum_{y<p\le x} \frac{|f(p)-g(p)|}{p} \Big).$$

We state a particular case of Theorem 3.

THEOREM 4: *Let f be a complex valued multiplicative function such that*

$$\sum_{p\le x} |f(p)| \ln p << x, \quad \sum_{p} \frac{|f(p)|^2}{p^2} \ln p < \infty,$$

$$(2.4)\quad \sum_{p\le x}\sum_{r=2}^{\infty} \frac{|f(p^r)|}{p^r} \ln p^r << (\ln\ln x)^2.$$

Assume that there is a sequence $g(p)$ *satisfying the conditions*

$$\sum_{p\le x} |g(p)| \ln p \ll x, \qquad \sum_{p} \frac{|g(p)|^2}{p^2} \ln p < \infty$$

and

$$\sum_{p\le x} g(p) \ln p = \tau x + O(x\, e^{-a\sqrt{\ln x}}), \tag{2.5}$$

where $\tau \in C$, $|\tau| \le c_4$ *and* $a > 0$ *and finally*

$$\sum_{p\le x} \frac{|f(p)-g(p)|}{p} \ln p \ll (\ln \ln x)^2. \tag{2.6}$$

Then with A *as in Theorem 1, the following asymptotical formula holds:*

$$\sum_{n\le x} f(n) = \frac{x \ln^{\tau-1} x}{\Gamma(\tau)} \prod_{p} (1-\frac{1}{p})^{\tau} (1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r}) (1 + O(\frac{\ln \ln x)^2}{\ln x})) +$$

$$+ O(x(\ln x)^{\max(0,\mathrm{Re}\,\tau-1)-1} (\ln \ln x)^{2(A-\max(0,\mathrm{Re}\,\tau-1))}). \tag{2.7}$$

3. SOME AUXILIARY RESULTS

To the proof of Theorem 1 we need the following facts.

LEMMA 1: *If* $f \in L$, *then we have*

$$\sum_{n \le x} |f(n)| \ll \frac{x}{\ln x} \prod_{|f|}(1,x).$$

A proof of this statement for the class W *is given in* [9], *Theorem 1. It is easy to check that the same proof works for the class* L.

LEMMA 2: *Let* g *be an exponentially multiplicative arithmetical function satisfying the conditions*

$$\sum_{p \le x} |g(p)| \ln p \ll x$$

and

$$\sum_{p \le x} g(p) \ln p = \tau x + O(x\,\rho(x)), \tag{3.1}$$

where $\tau \in C$, $|\tau| \le c_4$, $\rho(x) \downarrow 0$. *Then for* $y \le x$ *we have*

$$\sum_{\substack{n \le x \\ (n,\pi_y)=1}} g(n) = 1 + \int_1^{\ln x/\ln y} y^u z'(u)\,du + O\left(\frac{x\,\rho(y)}{\ln y}\left(\frac{\ln x}{\ln y}\right)^{A-1} \ln\frac{\ln x}{\ln y}\right),$$

where $z(t)$ $(t \geq 1)$ *is the solution of the differential-difference equation*

$$tz'(t) = \tau z(t-1)$$

under the initial condition $z(t) = 1$ $(0 \leq t \leq 1)$, *and* A *is assumed*

$$\sum_{u<p\leq z} \frac{|g(p)|}{p} \leq A \ln \frac{\ln z}{\ln u} + O(1).$$

This proposition is proved in [9] for the class W, and in [13] for exponentially multiplicative functions.

LEMMA 3: *Let* $z(t)$ $(t \geq 1)$ *be the solution of the differential difference equation*

$$tz'(t) = \tau z(t-1)$$

under the initial condition $z(t) = 1$ $(0 \leq t \leq 1)$. For $t \to \infty$ we have

$$z'(t) = \frac{e^{-c\tau}}{\Gamma(\tau)} t^{\tau-1} + (t^{\mathrm{Re}\ \tau-2});$$

$$z''(t) = O(t^{\mathrm{Re}\ \tau-2}).$$

For a proof of this lemma see [8], p. 139.

LEMMA 4: *Let* Q *be a finite set of primes, and let* (Q) *be the multiplicative semigroup generated by* Q. *Let* f *be a nonnegative multiplicative function such that the series* $\sum_{r=1}^{\infty} rf(p^r)$ *is convergent for every* $p \in Q$.

Then we have

$$\sum_{n\in(Q)} f(n) \ln n \leq \prod_{p\in Q} \left(1 + \sum_{r=1}^{\infty} f(p^r)\right) \sum_{p\in Q} \sum_{r=1}^{\infty} f(p^r) \ln p^r.$$

PROOF: *We have*

$$\sum_{n\in(Q)} f(n) \ln n = \sum_{n\in(Q)} f(n) \sum_{p^r \| n} \ln p^r = \sum_{p\in Q} \sum_{r=1}^{\infty} f(p^r) \ln p^r \sum_{\substack{n\in(Q) \\ (n,p)=1}} f(n).$$

From the assumptions of the lemma we obtain

$$\sum_{\substack{n\in(Q) \\ (n,p)=1}} f(n) \leq \sum_{n\in(Q)} f(n) = \prod_{p\in Q} \left(1 + \sum_{r=1}^{\infty} f(p^r)\right).$$

Substituting this into the previous equality we obtain the statement of the Lemma.

4. PROOF OF THEOREM 1

Denote $(\ln x)/(\ln y)$ by t. Then, according to Lemma 2, we have

$$\sum_{n\le x} h(n_y)\, f*g(n/n_y) = \sum_{\substack{n\le y^t \\ n\mid \pi_y}} h(n) \sum_{\substack{k\le y^t/n \\ (k,\pi_y)=1}} f(k) \sum_{\substack{m\le y^t/nk \\ (m,\pi_y)=1}} g(m) =$$

$$= \sum_{\substack{n\le y^t \\ n/\pi_y}} h(n) \sum_{\substack{k\le y^t/n \\ (k,\pi_y)=1}} f(k) +$$

$$+ \sum_{\substack{n\le y^t \\ n/\pi_y}} h(n) \sum_{\substack{k\le y^{t-1}/n \\ (k,\pi_y)=1}} f(k) \int_1^{t-\ln(kn)/\ln y} y^u z'(u)\,du +$$

$$+ O\Big(\frac{y^t}{\ln y}\, \Pi_{|h|}(1,y)\, \Pi_{|f|}(y,y^t)\rho(y)t^{A-1}\ln t\Big).$$

(4.1)

In view of Lemma 1 we have

$$\sum_{\substack{n\le y^t \\ n/\pi_y}} h(n) \sum_{\substack{k\le y^t/n \\ (k,\pi_y)=1}} f(k) \ll \frac{y^t}{t\ln y}\, \Pi_{|h|}(1,y)\, \Pi_{|f|}(y,y^t).$$

(4.2)

We estimate the second term in the right side of (4.1). With a change of variable and interchanging the integral and the summation we find

$$\sum_{\substack{n\le y^t \\ n/\pi_y}} h(n) \sum_{\substack{k\le y^t/n \\ (k,\pi_y)=1}} f(k) \int_1^{t-\ln(nk)-\ln y} y^u z'(u)\,du =$$

(4.3)

$$= \int_1^t y^u \sum_{\substack{n\le y^{u-1} \\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{u-1}/n \\ (k,\pi_y)=1}} \frac{f(k)}{k} z'(u - \frac{\ln nk}{\ln y})\,du.$$

We split the path of integration into two parts. The value of the integral from 1 to t/2 is small, we use a trivial estimate:

$$\int_1^{t/2} y^u \sum_{\substack{n\le y^{u-1} \\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{u-1}/n \\ (k,\pi_y)=1}} \frac{f(k)}{k} z'(u - \frac{\ln nk}{\ln y})\,du \ll$$

(4.4)

$$\ll \frac{y^{t/2}}{\ln y} t^{\max(0,\mathrm{Re}\,\tau-1)}\, \Pi_{|h|}(1,y)\, \Pi_{|f|}(y,y^t).$$

Denote the value of the integral from t/2 to t by 1. This will give us the main term; to estimate it we split the sum under the integral into three parts as follows:

$$\sum_{\substack{n\le y^{u-1}\\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{u-1/n}\\ (k,\pi_y)=1}} \frac{f(k)}{k}\, z'\Big(u-\frac{\ln nk}{\ln y}\Big)\,du =$$

$$= \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \sum_{\substack{k\, y^{t/4}/n\\ (k,\pi_y)=1}} + \sum_{\substack{y^{t/8}<n\le n^{u-1}\\ n/\pi_y}} \sum_{\substack{k\le y^{u-1}/n\\ (k,\pi_y)=1}} +$$

$$+ \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \sum_{\substack{\frac{y^{t/4}}{n}<k\le y^{u-1}/n\\ (k,\pi_y)=1}} .$$

We denote the values of the corresponding integrals by I_1, I_2, I_3. Applying Lemma 3 and taking into account that for I_1 we have $u > t/2$ and $(\ln(nk))/(\ln y) \le t/4$, we infer

$$I_1 = \int_{t/2}^{t} y^u \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{f(k)}{k}\, z'\Big(u-\frac{\ln nk}{\ln y}\Big)\,du =$$

$$= \frac{e^{-c\tau}}{\Gamma(\tau)} \int_{t/2}^{t} y^u \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{f(k)}{k}\Big(u-\frac{\ln nk}{\ln y}\Big)^{\tau-1} du +$$

$$+ O(t^{\mathrm{Re}\,\tau-2} \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{|h(n)|}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{|f(k)|}{k} \int_{t/2}^{t} y^u du) =$$

$$= \frac{e^{-c\tau}}{\Gamma(\tau)} \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{f(k)}{k} \int_{t/2}^{t} y^u u^{\tau-1} du +$$

$$+ O(\frac{1}{\ln y} \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{|h(n)|}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{f(k)}{k} \ln nk \int_{t/2}^{t} y^u u^{\mathrm{Re}\,\tau-2} du) +$$

$$+ O(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln y} \Pi_{|h|}(1,y)\, \Pi_{|f|}(y,y^t)) =$$

$$= \frac{e^{-c\tau}}{\Gamma(\tau)} (\Pi_h(1,y)\Pi_f(y,y^t) + O(\Pi_{|h|}(1,y) \sum_{\substack{y^{t/8}<k\le y^t\\ (k,\Pi y)=1}} \frac{|f(k)|}{k} +$$

$$+ |\Pi_f(y,y^t) \sum_{\substack{n>y^{t/8}\\ n/\pi_y}} \frac{h(n)}{n}|) (\frac{y^t t^{\tau-1}}{\ln y} + O(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln^2 y})) +$$

$$+ O\Big(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln^2 y} \sum_{\substack{n\le y^{t/8}\\ n/\pi_y}} \frac{|h(n)|}{n} \sum_{\substack{k\le y^{t/4}/n\\ (k,\pi_y)=1}} \frac{|f(k)|}{k} \ln nk\Big) +$$

$$+ O\Big(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln y}\Big) \Pi_{|h|}(1,y)\, \Pi_{|f|}(y,y^t)\Big).$$

Hence, after some transformations we obtain

$$I_1 = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{y^t t^{\tau-1}}{\ln y} \Pi_h(1,y)\Pi_f(y,y^t) +$$

$$+ O\Big(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln^2 y} \Pi_{|h|}(1,y) \sum_{\substack{(k,\pi_y)=1\\ k/\pi_{y^t}}} \frac{|f(k)|}{k} \ln k\Big) +$$

$$+ O\Big(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln^2 y} \Pi_{|f|}(y,y^t) \sum_{n/\Pi y} \frac{|h(n)|}{n} \ln n\Big) +$$

$$+ O\Big(\frac{y^t t^{\mathrm{Re}\,\tau-2}}{\ln y} \Pi_{|h|}(1,y)\Pi_{|f|}(y,y^t)\Big).$$

To the sums in the first and second remainder terms we apply Lemma 4. We obtain

$$I_1 = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{y^t\, t^{\tau-1}}{\ln y} \Pi_h(1,y)\Pi_f(y,y^t) +$$

$$+ O\Big(\frac{y^t\, t^{\operatorname{Re}\tau-2}}{\ln y} \Pi_{|h|}(1,y)\Pi_{|f|}(y,y^t)\Big(1+ \frac{1}{\ln y}\big(S_{|h|}(1,y) + \tag{4.5}$$

$$+ S_{|f|}(y,y^t)\big)\Big)\Big).$$

We estimate I_2. Using the estimate $z'(u) = O(u^{\max(0,\ \operatorname{Re}\tau-1)})$ and applying Lemma 4 we conclude

$$I_2 = \int_{t/2}^{t} y^u \sum_{\substack{y^{t/8}<n\le y^{u-1} \\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k\le y^{u-1}/n \\ (k,\pi_y)=1}} \frac{f(k)}{k} z'\Big(u - \frac{\ln nk}{\ln y}\Big)du =$$

$$= O\Big(\frac{y^t\, t^{\max(0,\operatorname{Re}\tau-1)-1}}{\ln^2 y} \Pi_{|h|}(1,y)\Pi_{|f|}(y,y^t)S_{|h|}(1,y)\Big). \tag{4.6}$$

Analogously we derive the estimate

$$I_3 = \int_{t/2}^{t} y^u \sum_{\substack{n\le y^{t/8} \\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{y^{t/4}/n<k\le y^{u-1}/n \\ (k,\pi_y)=1}} \frac{f(k)}{k} z'\Big(u - \frac{\ln nk}{\ln y}\Big)du =$$

$$= O\Big(\frac{y^t\, t^{\max(0,\operatorname{Re}\tau-1)-1}}{\ln^2 y} \Pi_{|h|}(1,y)\Pi_{|f|}(y,y^t)S_{|f|}(y,y^t)\Big). \tag{4.7}$$

By virtue of $I = I_1 + I_2 + I_3$, from (4.5)-4.7) we infer

$$\int_{t/2}^{} y^u \sum_{\substack{n \le y^{u-1} \\ n/\pi_y}} \frac{h(n)}{n} \sum_{\substack{k \le y^{u-1}/n \\ (k,\pi_y)=1}} \frac{f(k)}{k} z'(u - \frac{\ln nk}{\ln y}) du =$$

$$= \frac{e^{-c\tau}\, y^t\, t^{\tau-1}}{\Gamma(\tau)\ \ln y}\ \Pi_h(1,y)\Pi_f(y,y^t) +$$

(4.8)

$$+\ O\Big(\frac{y^t}{\ln y}\, t^{\max(0,\mathrm{Re}\,\tau-1)-1}\Big)\Pi_{|h|}(1,y)\Pi_{|f|}(y,y^t)$$

$$\Big(1 + \frac{S_{|h|}(1,y)+S_{|f|}(y,y^t)}{\ln y}\Big)\Big).$$

Taking into account that the integral on $[1, t/2]$ is absorbed by the remainder term of (4.8) by (4.4), we conclude that the expression on the left side of (4.3) is equal to the right side of (4.8). Substituting (4.3) and (4.2) into (4.1) we obtain (2.2).
This concludes the proof of Theorem 1.

5. PROOF OF THEOREM 2

The sequence $g(p)$ determines an exponentially multiplicative function $g(n)$ uniquely. The set of

multiplicative arithmetical functions under the operation of the Dirichlet convolution forms a commutative group, the unity of which is the function

$$E(n) = \begin{cases} 1 & \text{for } n = 1, \\ 0 & \text{for } n \neq 1. \end{cases}$$

Therefore for given multiplicative functions f and g one can find a unique multiplicative function f_0 such that $f = f_0 * g$, namely $f_0 = f*\tilde{g}$, where $\tilde{g}$ is the inverse function of g with respect the operation $*$. Observe that $\tilde{g}(p) = -g(p)$ and $\tilde{g}(p^r) = (-g(p))^r/r!$

Since in the case considered we have $|h(n)| \leq 1$, we have obviously

$$(5.1) \qquad S_{|h|}(1,y) = \sum_{p\leq y} \sum_{r=1}^{\infty} \frac{|h(p^r)|}{p^r} \ln p^r \ll \ln y,$$

$$(5.2) \qquad \Pi_h(1,y) = \prod_{p\leq y} (1 + \sum_{r=1}^{\infty} \frac{|h(p^r)|}{p^r}) \ll \prod_{p\leq y} (1 + \frac{|h(p)|}{p}).$$

It is easy to chek that $|\tau| \leq 1$ and

$$(5.3) \qquad S_{|f*\tilde{g}|}(y,x) \ll 1 + \sum_{y<p\leq x} \frac{|f(p)-g(p)|}{p} \ln p,$$

$$(5.4)\qquad \Pi_{|f*\tilde{g}|}(y,x) \ll \exp \sum_{y<p\le x} \frac{|f(p)-g(p)|}{p}\,.$$

According to the above observations, applying Theorem 1 we conclude

$$\sum_{n\le x} h(n_y) f(n/n_y) = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{x}{\ln x} \left(\frac{\ln x}{\ln y}\right)^{\tau} \Pi_h(1,y)\Pi_{f*\tilde{g}}(y,x) +$$

$$+ O\Big(\frac{x}{\ln x}\,\Pi_{|h|}(1,y)\Pi_{|f*\tilde{g}|}(y,x)\Big(\rho(y)\Big(\frac{\ln x}{\ln y}\Big)^{A} \ln\frac{\ln x}{\ln y} +$$

$$+ 1 + \frac{1}{\ln y}\big(S_{|h|}(1,y) + S_{|f*\tilde{g}|}(y,x)\big)\Big)\Big).$$

Hence in view of (5.1)-(5.4) we obtain

$$(5.5)\qquad \sum_{n\le x} h(n_y) f(n/n_y) = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{x}{\ln x} \left(\frac{\ln x}{\ln y}\right)^{\tau} \Pi_h(1,y)\Pi_{f*\tilde{g}}(y,x) +$$

$$+ O\Big(\frac{x}{\ln x}\Big(\ (y)\Big(\frac{\ln x}{\ln y}\Big)^{A} \ln\frac{\ln x}{\ln y} + 1 + \frac{1}{\ln y} \sum_{y<p\le x} \frac{|f(p)-g(p)|}{\ln p}\Big)\times$$

$$\times \exp\Big(\sum_{p\le y} \frac{|h(p)|}{p} + \sum_{y<p\le x} \frac{|f(p)-g(p)|}{p}\Big).$$

We transform the main term of this formula. Since $|f(n)| \le 1$ and $|\tilde{g}(n)| \le 1$, it is easy to see that

$$\Pi_{f*\tilde{g}}(y,x) = \Pi_f(y,x)\Pi_{\tilde{g}}(y,x).$$

Further, according to (2.1), under the assumption that $y = y(x)$ satisfies

$$\int_y^x \rho(u)\, d \ln \ln u = O(1),$$

we find

$$\sum_{y<p\le x} \frac{g(p)}{p} = -\int_y^x \sum_{p\le u} g(p) \ln p \frac{\ln u+1}{u^2 \ln^2 u} du + \frac{1}{x \ln x} \sum_{p\le x} g(p) \ln p -$$

$$- \frac{1}{y \ln y} \sum_{p\le y} g(p) \ln p = \tau \ln \frac{\ln x}{\ln y} + O\left(\int_y^x \rho(u) d \ln \ln u\right) +$$

$$+ O\left(\frac{(y)}{\ln y}\right),$$

and hence

$$(5.6)\quad \Pi_{\tilde{g}}(y,x) = \exp\left(- \sum_{y<p\le x} \frac{g(p)}{p}\right) = \left(\frac{\ln y}{\ln x}\right)^{\tau} \left(1 + O\left(\frac{\rho(y)}{\ln y}\right) +\right.$$

$$+O\Big(\int_y^x \rho(u)\,d\ln\ln u\Big)\Big) = \Big(\frac{\ln y}{\ln x}\Big)^{\tau}\Big(1+O\Big(\rho(u)\ln\frac{\ln x}{\ln y}\Big)\Big).$$

Taking into account (5.2) and

$$\Pi_f(y,x) \ll \Big(\frac{\ln x}{\ln y}\Big)^{A}\exp\sum_{y<p\le x}\frac{|f(p)-g(p)|}{p}$$

it is easy to show that the new error term arising at the substitution of (5.6) into (5.5) is absorbed by the other one. This finishes the proof of Theorem 2.

6. PROOF OF THEOREM 3

According to the remarks made at the beginning of the previous section we may apply Theorem 1 to infer

$$\sum_{n\le x} h(n_y)f(n/n_y) = \frac{e^{-C\tau}}{\Gamma(\tau)}\frac{x}{\ln x}\Big(\frac{\ln x}{\ln y}\Big)^{\tau}\Pi_h(1,y)\Pi_{f*\tilde{g}}(y,x)$$

$$(6.1)\qquad + O\Big(\frac{x}{\ln x}\Pi_{|h|}(1,y)\Pi_{|f*\tilde{g}|}(y,x)\Big(\rho(y)\Big(\frac{\ln x}{\ln y}\Big)^{A}\ln\frac{\ln x}{\ln y} +$$

$$+ \Big(\frac{\ln x}{\ln y}\Big)^{\max(0,\mathrm{Re}\,\tau-1)}\Big(1+\frac{1}{\ln y}\big(S_{|h|}(1,y)+S_{|f*\tilde{g}|}(y,x)\big)\Big)\Big)\Big).$$

We estimate $S_{|f*\tilde{g}|}(y,x)$.

$$S_{|f*\tilde{g}|}(y,x) = \sum_{y<p\le x} \sum_{r=1}^{\infty} \Big| \sum_{k+l=r} f(p^k) \frac{(-g(p))^l}{l!} \frac{\ln p^r}{p^r} \le$$

$$\le \sum_{y<p\le x} \Big(\frac{|f(p)-g(p)|}{p} \ln p + \sum_{k+l\ge 2} \frac{|f(p^k)|}{p^k} \frac{|g(p)|^l}{l!\, p^l} \ln p^{k+l} \Big) \le$$

$$\le \sum_{y<p\le x} \frac{|f(p)-g(p)|}{p} \ln p + \sum_{y<p\le x} \sum_{k=2}^{\infty} \frac{|f(p^k)|}{p^k} \ln p^k \sum_{l=2}^{\infty} \frac{|g(p)|^l}{l!\, p^l} \ln p^l +$$

$$+ \sum_{y<p\le x} \Big(1 + \frac{2|g(p)|}{p}\Big) \sum_{k=2}^{\infty} \frac{|f(p^k)|}{p^k} \ln p^k +$$

$$+ \sum_{y<p\le x} \Big(1 + \frac{2|f(p)|}{p}\Big) \sum_{l=2}^{\infty} \frac{|g(p)|^l}{l!\, p^l} \ln p^l + \sum_{y\, p\, x} \frac{|f(p)||g(p)|}{p^2} \ln p^2.$$

From the assumptions of the theorem it follows that the last two terms are $o(1)$, and the second and the third ones are

$$O\Big(\sum_{y<p\le x} \sum_{k=2}^{\infty} \frac{|f(p^k)|}{p^k} \ln p^k \Big).$$

Consequently

$$(6.2)\qquad S_{|f*\tilde{g}|}(y,x) \ll 1 + \sum_{y<p\le x}\Big(\frac{|f(p)-g(p)|}{p}\ln p + \sum_{r=2}^{\infty}\frac{|f(p^r)|}{p^r}\ln p^2\Big).$$

Further, it is easy to show that for $p \to \infty$ we have

$$\sum_{r=1}^{\infty}|f*\tilde{g}(p^r)|p^{-r} \to 0,$$

hence for $p > y$ we have

$$\ln\Big(1 + \sum_{r=1}^{\infty}\frac{|f*\tilde{g}(p^r)|}{p^r}\Big) = \frac{|f(p)-g(p)|}{p} +$$

$$(6.3)\qquad + O\Big(\sum_{r=2}^{\infty}\frac{1}{p^r}\sum_{k+l=r}|f(p^k)|\frac{|g(p)|^l}{l!}\Big).$$

The expression in the O is at most

$$\Big(1 + \frac{|g(p)|}{p}\Big)\sum_{k=2}^{\infty}\frac{|f(p^k)|}{p^k} + \Big(1 + \frac{|f(p)|}{p}\Big)\sum_{l=2}^{\infty}\frac{|g(p)|^l}{l!\,p^l} +$$

$$+ \frac{|f(p)||g(p)|}{p^2} + \sum_{k=2}^{\infty}\frac{|f(p^k)|}{p^k}\sum_{l=2}^{\infty}\frac{|g(p)|^l}{l!\,p^l}.$$

Consequently, summing over p in the interval $y<p\le x$, using the assumptions of the theorem and applying Cauchy's inequality we find

$$\sum_{y<p\le x} O\Big(\sum_{r=2}^{\infty}\frac{1}{p^r}\sum_{k+l=r}|f(p^k)|\frac{|g(p)|^l}{l!}\Big) \ll \sum_{y<p\le x}\sum_{k=2}^{\infty}\frac{|f(p^k)|}{p^k} +$$

$$+\sum_{y<p\le x}\frac{|g(p)|^2}{p^2}+\sqrt{\sum_{y<p\le x}\frac{|f(p)^2|}{p^2}\sum_{y<p\le x}\frac{|g(p)^2|}{p^2}} = o(1).$$

Therefore from this and (6.3) we infer

$$(6.4)\qquad \Pi_{|f*\tilde{g}|}(y,x) \ll \exp\sum_{y<p\le x}\frac{|f(p)-g(p)|}{p}.$$

To complete the proof we need to substitute (6.2), (6.4) and the relation

$$\Pi_{f*\tilde{g}}(y,x) = \Pi_f(x,y)\Big(\frac{\ln y}{\ln x}\Big)^{\tau}\Big(1+O\big(\rho(y)\ln\frac{\ln x}{\ln y}\big)\Big)$$

to (6.1), and repeat the arguments from the end of §5.

7. PROOF OF THEOREM 4

Under the assumptions, the conditions of Theorem 3 are fulfilled with $h = f$ $\rho(x) = \exp(-a\sqrt{\ln x})$. Since the series

$$\sum_p |f(p)-g(p)|p^{-1}, \quad \sum_p \sum_{r\geq 2} |f(p^r)|p^{-r}$$

converge and

$$\sum_{p\leq y} |g(p)|p^{-1} \leq A \ln\ln y + O(1),$$

we have $\Pi_{|f|}(1,y) \ll \ln^A y$. Besides, from the conditions of the theorem it follows that

$$\sum_{p\leq y} \sum_{r=1}^{\infty} |f(p^r)|p^{-r} \ln p^r \ll \ln y.$$

Hence (2.3) in this case will have the form

$$\sum_{n\leq x} f(n) = \frac{e^{-c\tau}}{\Gamma(\tau)} \frac{x}{\ln x} \Pi_f(1,x) + O\Big(\frac{x}{\ln x}\Big(e^{-a\sqrt{\ln y}}(\ln^A x)\ln\frac{\ln x}{\ln y} + \tag{7.1}$$

$$+ (\ln x)^{\max(0,\operatorname{Re}\tau-1)}(\ln y)^{A-\max(0,\operatorname{Re}\tau-1)}\Big(1 + \frac{(\ln\ln x)^2}{\ln y}\Big)\Big)\Big).$$

We choose y so that both terms in the remainder have the same order of magnitude. To this end we put

$$y = \exp\left(\left(\frac{A-\max(0,\operatorname{Re}\,\tau-1)}{a}\right)^2 (\ln\ln x + \left(\frac{1}{A-\max(0,\operatorname{Re}\,\tau-1)} - 2\right)\ln\ln\ln x)^2\right).$$

Then the remainder term of this asymptotical formula becomes

$$(7.2)\quad O\left(\frac{x}{\ln x}(\ln x)^{\max(0,\operatorname{Re}\,\tau-1)}(\ln\ln x)^{2(A-\max(0,\operatorname{Re}\,-1))}\right).$$

Further, since $f(p) = o(p)$ and $\sum_{r\geq 2} \frac{|f(p^r)|}{p^r} = o(1)$, we find

$$\prod_{p\geq x}(1 - \frac{1}{p})^{\tau}(1 + \sum_{r=1}^{\infty}\frac{f(p^r)}{p^r}) =$$

$$= \exp\lim_{z\to\infty}\sum_{x<p\leq z}\left(\frac{f(p)-g(p)}{p} + \frac{g(p)-\tau}{p} + O\left(\sum_{r=2}^{\infty}\frac{|f(p^r)|}{p^r} + \frac{1}{p^2}\right)\right).$$

By virtue of (2.4) and (2.6) we have

$$\sum_{x<p\leq z}\left(\frac{|f(p)-g(p)|}{p} + O\left(\sum_{r=2}\frac{|f(p^r)|}{p^r} + \frac{1}{p^2}\right)\right) = O\left(\frac{\ln\ln x}{\ln x}\right),$$

and from (2.5) we conclude

$$\sum_{x<p\le z} \frac{g(p)-}{p} = O(e^{-a_1\sqrt{\ln x}}), \qquad a_1 > 0.$$

Hence, applying Mertens' theorem ([12], p. 94) we obtain

$$\Pi_f(1,x) = \prod_p (1 + \sum_{r=1}^{\infty} \frac{\xi(p^r)}{p^r})(1 - \frac{1}{p})^{\tau} \prod_{p\le x} (1 - \frac{1}{p})^{-\tau} \times$$

$$\times \Big(\prod_{p>x} (1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r})(1 - \frac{1}{p})^{\tau} \Big)^{-1} =$$

$$= \prod_p (1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r})(1 - \frac{1}{p})^{\tau} e^{c\tau} \ln x \left(1 + O\left(\frac{(\ln \ln x)^2}{\ln x}\right)\right).$$

From (7.1-(7.3) we deduce

$$\sum_{n\le x} f(n) = \frac{x \ln^{-1} x}{\Gamma(\tau)} \prod_p (1 + \sum_{r=1}^{\infty} \frac{f(p^r)}{p^r})(1 - \frac{1}{p})^{\tau} \left(1 + O\left(\frac{\ln \ln x)^2}{\ln x}\right)\right) +$$

$$+ O(x(\ln x)^{\max(0,\mathrm{Re}\,\tau-1)-1} (\ln \ln x)^{2(A-\max(0,\mathrm{Re}\,\tau-1))}),$$

qu. e.d.

REFERENCES

[1] HALÁSZ, G., *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hung. 19 (1968), 365-403.

[2] KRYZIUS, Z.A., Mean values of multiplicative functions, (in Russian). *Liet. Mat. Rinkinys* 20 (1980), No. 2, 69-78.

[3] KUBILIUS, J.P., The method of Dirichlet generating series in the theory of distribution of additive arithmetical functions I. (in Russian), *Liet. Mat. Rinkinys* 11 (1971), No. 1, 125-134.

[4] LAURINCIKAS, A.P., Large deviations of arithmetical functions, (in Russian), *Liet. Mat. Rinkinys* 16 (1976), No. 1, 159-171.

[5] LEVIN, B.V., TIMOFEEV, N.M., On sums of multiplicative functions, (in Russian), *Doklady Acad. Sci.* USSR 193 (1970), No. 5, 992-995.

[6] LEVIN, B.V., TIMOFEEV, N.M., Sums of multiplicative functions, (in Russian), *Studia Sci. Math. Hung.* 18 (1983), 21-41.

[7] LEVIN, B.V., FAINLEIB, A.S., On a method of summation of multiplicative functions, (in Russian), *Izv. Acad. Sci.* USSR, Ser. mat. 31 (1967), 691-710.

[8] LEVIN, B.V., FAINLEIB, A.S., *An application of certain integral equations to problems of number theory*, (in Russian), Uspekhi Matem. Nauk 22 (1967), No. 3, 119-197.

[9] LEVIN, B.V., FAINLEIB, A.S., Multiplicative functions and probabilistic number theory, (in Russian), *Izv. Acad. Sci.* USSR, Ser. mat. 5 (1970), 1064-1109.

[10] MANSTAVIČIUS, E., An application of the method of Dirichlet generating series to the theory of distribution of values of arithmetical functions, (in Russian), *Liet. Mat. Rinkinys* 14 (1974), 99-111.

[11] PARSON, A., TULL, J., Asymptotic behabior of multiplicative functions, *J. Number Theory* 10 (1978), 395-420.

[12] PRACHAR, K., *Primzahlverteilung*, Springer, Berlin 1957.

[13] TULYAGANOV, S.T., Asymptotics for the mean values of multiplicative functions, (in Russian), *Mat. Zametki* 38 (1985), No. 1., 15-28.

[14] TULYAGANOV, S.T., On the mean values of multiplicative functions on an arithmetical progression, (in Russian), *Mat. Zametki* 42 (1987), No. 2., 315-334.

[15] WIRSING, E., Das asymptotische Verhalten von Summen über multiplikative Funktionen, *Math. Ann.* 143 (1961), 75-102.

[16] WIRSING, E., Das asymptotische Verhalten von Summen über multiplikative Funktionen II, *Acta Math. Sci. Hung.* 18 (1967), 411-467.

TULYAGANOV, S.T.

Institut Matematiky
AN Y3 SSR
ul. F. Hodnajeva 29
700143 TASKENT, Akadem Gorod
U S S R



1346-2 a

K. GYŐRY
and
G. HALÁSZ
editors

NUMBER THEORY Vol. I.

MC
109.747/1