COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

ON A CLASS OF ARITHMETICAL CONVOLUTIONS

BY

W. NARKIEWICZ (WROCŁAW)

1. Let us associate with every natural number n a set A_n of divisors of the number n. We can now define with the aid of the formula

$$h(n) = \sum_{d \in A_n} f(d) g\left(\frac{n}{d}\right) \tag{1}$$

a convolution $f * g = h$ of two arithmetical functions. In the case when A_n is the set of all divisors of the number n, (1) defines the classical Dirichlet convolution, and in the case, when A_n is the set of all unitary divisors of the number n, i. e. $A_n = \{d: (d, n/d) = 1\}$, (1) defines the unitary convolution introduced by Cohen ([2], [3]). The set of all complex-valued arithmetical functions with ordinary addition, and with multiplication defined by (1) forms a ring R_A, in general non-associative and non-commutative.

In this paper we shall be concerned with a class of convolutions which preserve multiplicativity, and for which the ring R_A is commutative, associative, and has a unit element. Moreover, the inverse function of $f(n) \equiv 1$ shall assume for prime powers only the values 0 and -1. (The last condition in the case of Dirichlet and unitary convolution is a well-known property of the function of Möbius resp. of Liouville). If a convolution has the above listed properties we shall say it is a *regular convolution*.

First we establish the conditions which should be imposed upon the sets A_n to get the associativity, commutativity, and some other properties of the ring R_A. We shall prove a theorem characterizing the regular convolutions, and we shall show that some results of E. Cohen, regarding the unitary convolution can be proved in more general cases also.

Finally we shall examine the subring B_A of R_A consisting of all functions $f(n)$ satisfying $\|f\| = \sum_{n=1}^{\infty} |f(n)| < \infty$. It turns out that B_A is a normed algebra; we shall identify the maximal ideals of B_A and shall solve the problem of homeomorphism of the spaces of maximal ideals belonging to different B_A. As an easy corollary we obtain that, in unitary convolution, if $\sum_{n=1}^{\infty}|f(n)| < \infty$, $f(1) \neq 0$, and $g(n)$ is the inverse function to $f(n)$, then $\sum_{n=1}^{\infty}|g(n)| < \infty$.

2. (i) *The ring R_A is associative if and only if the following two conditions are equivalent*:

(a) $d \in A_m$, $m \in A_n$,

(b) $d \in A_n$; $m/d \in A_{n/d}$.

Proof. Let us define, for $k = 1, 2, \ldots$,

$$e_k(n) = \begin{cases} 1 & \text{if} \quad n = k, \\ 0 & \text{if} \quad n \neq k. \end{cases}$$

Then, for all f, $f(n) = \sum_{k=1}^{\infty} f(k) e_k(n)$.

From (1) it follows that

$$(f*g)*h = \sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\sum_{m=1}^{\infty} f(k)g(l)h(m)[(e_k*e_l)*e_m],$$

$$f*(g*h) = \sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\sum_{m=1}^{\infty} f(k)g(l)h(m)[e_k*(e_l*e_m)];$$

hence the convolution will be associative if and only if $(e_k*e_l)*e_m = e_k*(e_l*e_m)$ for every k, l, m. An easy computation shows that $[(e_k*e_l)*e_m](n) = 1$ if $n = klm$, $k \in A_{kl}$, $kl \in A_n$, and is equal to zero in the remaining cases. Similarly, $[e_k*(e_l*e_m)](n) = 1$ if $n = klm$, $k \in A_n$, $l \in A_{lm}$, and is equal to zero in the remaining cases. By putting now $d' = k$, $m' = kl$, $n' = klm$, we obtain the required equivalence.

(ii) *The ring R_A is commutative if and only if from $d \in A_n$ it follows that $n/d \in A_n$.*

Proof. The sufficiency is evident. If R_A is commutative and there exists a pair d, n, such that $d \in A_n$, but $n/d \notin A_n$, then

$$1 = (e_d * e_{n/d})(n) = (e_{n/d} * e_d)(n) = 0,$$

a contradiction.

(iii) *The ring R_A has a unit element if and only if for every n, $\{1, n\} \subset A_n$.*

Proof. If $\{1, n\} \subset A_n$, then $e_1 * f = f * e_1 = f$ for all f; hence e_1 is the unit element. Suppose now that R_A has a unit element l, and there exists an integer k, such that $k \notin A_k$. Then $1 = e_k(k) = (e_k * l)(k) = \sum_{d \in A_k} e_k(d) l(k/d) = 0$, a contradiction. Similarly, if $1 \notin A_k$, then

$$1 = e_k(k) = (l * e_k)(k) = \sum_{d \in A_k} l(d) e_k(k/d) = 0,$$

a contradiction.

It should be remarked that if R_A has a unit element l, then $l = e_1$. Moreover, the set of elements which have the inverse in R_A is the same for all R_A with a unit element, namely it is the set of all functions $f(n)$ non-vanishing at $n = 1$. This is easy to establish, for if f has an inverse f^{-1}, then $1 = (f * f^{-1})(1) = f(1) f^{-1}(1)$, and so $f(1) \neq 0$. Conversely, if $f(1) \neq 0$, then we can define $f^{-1}(n)$ by induction:

$$f^{-1}(1) = 1/f(1); \quad f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d \in A_n \\ d > 1}} f(d) f^{-1}(n/d).$$

As usually, we shall say that a *function* $f(n) \not\equiv 0$ *is multiplicative* if $f(mn) = f(m)f(n)$ for $(m, n) = 1$. We shall say that the *convolution is multiplicative* if from the multiplicativity of the factors follows the multiplicativity of the convolution product.

(iv) *The convolution defined by* (1) *is multiplicative if and only if* $A_{mn} = A_m \times A_n$ *for* $(m, n) = 1$.

(Here $B \times C$ denotes the set of all integers, which can be represented in the form bc, $b \in B$, $c \in C$).

Proof. If f and g are multiplicative functions, $(m, n) = 1$, $A_{mn} = A_m \times A_n$, and $h = f * g$, then

$$h(mn) = \sum_{d \in A_{mn}} f(d) g(mn/d) = \sum_{\substack{d_1 | m \\ d_2 | n \\ d_1 d_2 \in A_{mn}}} f(d_1) f(d_2) g(m/d_1) g(n/d_2)$$

$$= \sum_{d_1 \in A_m} f(d_1) g(m/d_1) \cdot \sum_{d_2 \in A_n} f(d_2) g(n/d_2) = h(m) h(n).$$

Conversely, let $(m, n) = 1$ and for all multiplicative functions f, g, $h(mn) = h(m)h(n)$, where $h = f * g$. If we define $d_k(x) = x^k * 1$, then $d_k(mn) = d_k(m) d_k(n)$ for all k; hence

$$\sum_{d \in A_{mn}} d^k = d_k(mn) = d_k(m) d_k(n) = \sum_{d \in A_m} \sum_{D \in A_n} (dD)^k \tag{2}$$

$$= \sum_{\substack{d = d_1 \cdot d_2 \\ d_1 \in A_m, d_2 \in A_n}} d^k = \sum_{d \in A_m \times A_n} d^k,$$

for from $(m, n) = 1$ it follows that the products dD ($d \in A_m$, $D \in A_n$) are all different.

Let now

$$A_{mn} = \{d_1 < d_2 < \ldots < d_r\}, \qquad A_m \times A_n = \{\delta_1 < \delta_2 < \ldots < \delta_{r_1}\}.$$

As $d_0(x) = \overline{\overline{A}}_x$, we have $r = r_1$.

From (2) we obtain:

$$d_1^k + \ldots + d_r^k = \delta_1^k + \ldots + \delta_r^k$$

for $k = 1, 2, \ldots$ If now $A_{mn} \neq A_m \times A_n$, then let i be the greatest index such that $d_i \neq \delta_i$. If $d_i < \delta_i$, then

$$\delta_i^k \leqslant \delta_1^k + \ldots + \delta_i^k = d_1^k + \ldots + d_i^k \leqslant i \cdot d_i^k \quad \text{and} \quad \left(\frac{d_i}{\delta_i}\right)^k \geqslant \frac{1}{i} > 0.$$

But this is impossible, if k is sufficiently large. The case $d_i > \delta_i$ can be dealt with in the same way. The obtained contradiction shows that $A_{mn} = A_m \times A_n$.

From (iv) it follows that if $A_{mn} = A_m \times A_n$ for $(m, n) = 1$, then the multiplicative functions form a semigroup with respect to the convolution. In the case of unitary convolution this has been noticed by Cohen ([3], th. 2.1). We shall now prove

(v) *If the ring R_A is associative, has a unit element, and the multiplicative functions form a semigroup, then they form a group.*

Proof. It is sufficient to prove that if f is multiplicative, then f^{-1} is also multiplicative. (The existence of f^{-1} follows from the fact that $f(1) = 1$, and from the remark after (iii)). Evidently $f^{-1}(1) = 1$. Suppose that for $r < k$ from $r = r_1 r_2$, $(r_1, r_2) = 1$ it follows that $f^{-1}(r) = f^{-1}(r_1) f^{-1}(r_2)$. Let $k = mn$, $(m, n) = 1$, $m, n \neq 1$. Then

$$0 = \sum_{d \in A_{mn}} f(d) f^{-1}(mn/d) = \sum_{\delta_1 \in A_m} \sum_{\delta_2 \in A_n} f(\delta_1) f(\delta_2) f^{-1}(mn/\delta_1 \delta_2)$$
$$= \sum_{\substack{\delta_1 \in A_m \\ \delta_1 \delta_2 \neq 1}} \sum_{\delta_2 \in A_n} \{f(\delta_1) f(\delta_2) f^{-1}(m/\delta_1) f^{-1}(n/\delta_2)\} + f^{-1}(mn).$$

But

$$0 = \sum_{\delta_1 \in A_m} f(\delta_1) f^{-1}(m/\delta_1) \cdot \sum_{\delta_2 \in A_n} f(\delta_1) f^{-1}(n/\delta_2)$$
$$= \sum_{\substack{\delta_1 \in A_m \\ \delta_1 \cdot \delta_2 \neq 1}} \sum_{\delta_2 \in A_n} \{f(\delta_1) f(\delta_2) f^{-1}(m/\delta_1) f^{-1}(n/\delta_2)\} + f^{-1}(m) f^{-1}(n).$$

By comparing these equalities we obtain $f^{-1}(mn) = f^{-1}(m) f^{-1}(n)$.

The statement (v) can be also formulated in the following, evidently equivalent form:

(v') *If the ring R_A is associative, has a unit element, and is multiplicative, the function f is multiplicative, and $f = g * h$, then either both the functions g, h, are multiplicative, or both of them are not.*

In this form it has been proved in the case of Dirichlet convolution by Bell ([1]).

3. Let us now define: the convolution A defined by (1) is *regular* if it satisfies the following conditions:

(a) The ring R_A is associative, commutative, and possesses a unit element.

(b) The convolution preserves multiplicativity.

(c) The "Möbius-function" of the convolution A, defined by the equation $1 * \mu_A = e_1$, assumes for prime powers only the values 0 and -1.

(The multiplicativity of μ_A follows from (b) and (v). In the case of Dirichlet convolution μ_A is the ordinary Möbius function, and in the case of unitary convolution it is the Liouville function).

We shall say that the number n is *A-primitive* (or briefly: *primitive*, if A is fixed), if $A_n = \{1, n\}$. In the case of Dirichlet convolution primitive numbers are the primes, and in the unitary case primitive numbers are the prime powers. From (b) and (iv) we obtain that in a regular convolution every primitive number must be a prime power, but the converse implication is true in the unitary case only. The question can be posed whether the set of primitive numbers determines the regular convolution uniquely. We shall see later that in general this is not the case.

THEOREM I. *The convolution satisfying* (a) *and* (b) *is regular if and only if for every prime power p^k the set A_{p^k} is of the form: $1, p^t, p^{2t}, \ldots, p^{rt} = p^k$, with some $t \neq 0$, and, moreover, $p^t \in A_{p^{2t}}, p^{2t} \in A_{p^{3t}}, \ldots$*

Proof. Suppose, the convolution is regular. First we prove that

$$\mu_A(p^a) = \begin{cases} -1 & \text{if} \quad p^a \text{ is primitive}, \\ 0 & \text{if} \quad p^a \text{ is not primitive}. \end{cases} \tag{3}$$

If p^a is primitive, then $0 = (\mu_A * 1)(p^a) = \mu_A(p^a) + 1$; hence $\mu_A(p^a) = -1$.

If now p^a is an arbitrary prime power, and $A_{p^a} = \{1, p^{a_1}, \ldots, p^{a_r}\}$, where $0 < a_1 < \ldots < a_r = a$, then it is clear that p^{a_1} must be primitive, and so

$$0 = (\mu_A * 1)(p^a) = 1 + \mu_A(p^{a_1}) + \sum_{j=2}^{r} \mu_A(p^{a_j}) = \sum_{j=2}^{r} \mu_A(p^{a_j});$$

whence no one of the p^{a_j} $(j \geqslant 2)$ can be primitive and, moreover, $\mu_A(p^{a_j}) = 0$ $(j \geqslant 2)$. So (3) is proved and we see that in A_{p^a} there can be one primitive number only.

Let us now observe that $p^{a_1} \epsilon A_{p^{a_2}}$, since p^{a_2} is not primitive, and from (a) and (i) it follows that in every set A_n there must be a primitive number (namely, the least number in A_n different from 1). From this we obtain that $p^{a_2-a_1} \epsilon A_{p^{a_2}}$ (by (ii)), but as $p^{a_2-a_1} < p^{a_2}$, we must have $a_2 = 2a_1$, for $p^{a_2-a_1} \epsilon A_{p^a}$. An easy induction leads us to $a_k = ka_1$ $(k \leqslant r)$, and $p^{a_k} \epsilon A_{p^{a_{k+1}}}$ $(k = 1, \ldots, r-1)$, which proves the first part of the theorem. The second part of the theorem can be easily checked by computing the values of the function $\mu_A(n)$ for prime powers.

THEOREM II. *Let K be the class of all decompositions of the set of non-negative integers into arithmetical progressions (finite or not), containing zero, and such that no two progressions belonging to the same decomposition have a positive number in common. Let us associate with every prime number p an element π_p of K. Let the sets A_n be defined by:*

$$\prod p_i^{a_i} \epsilon A_m, \quad \textit{where} \quad m = \prod p_i^{\beta_i},$$

if and only if for every i: $a_i \leqslant \beta_i$, and a_i, β_i belong in the decomposition π_{p_i} to the same progression. Then these sets A_n define a regular convolution, and conversely every regular convolution can be obtained in this way.

Proof. Let us write $\langle a, \beta\rangle_i$ if in the decomposition π_{p_i} the numbers a, β belong to the same progression. Let $d = \prod p_i^{a_i}$, $m = \prod p_i^{\beta_i}$, $n = \prod p_i^{\gamma_i}$. If $d \epsilon A_m$, $m \epsilon A_n$, then $a_i \leqslant \beta_i \leqslant \gamma_i$, $\langle a_i, \beta_i\rangle_i$, $\langle \beta_i, \gamma_i\rangle_i$; hence $\langle a_i, \gamma_i\rangle_i$, i. e. $d \epsilon A_n$. Moreover, from $\langle a_i, \beta_i\rangle_i$ it follows that $\langle a_i, \beta_i - a_i\rangle_i$; similarly $\langle a_i, \gamma_i - a_i\rangle_i$. Hence $\langle \beta_i - a_i, \gamma_i - a_i\rangle_i$, i. e. $m/d \epsilon A_{n/d}$.

If $d \epsilon A_n$, $m/d \epsilon A_{n/d}$, then it is easy to verify that $d \epsilon A_m$, and $m \epsilon A_n$, by proceeding similarly as above. Hence the associativity of the convolution is obtained.

The commutativity, existence of the unit element, and the multiplicativity follow at once from the definition of A_n. Hence the conditions (a), (b), are verified and now the application of the theorem I proves the first part of the theorem.

Conversely, let the sets A_n define a regular convolution. Then we can associate with every prime number p a decomposition of the set of non-negative integers putting two integers m and n $(m \leqslant n)$ to the same class if and only if $p^m \epsilon A_{p^n}$. From theorem I it follows that these decompositions belong to the class K, and from (b) and (iv) we get moreover, that $\prod p_i^{a_i} \epsilon A_m$, if and only if, for every i, $a_i \leqslant \beta_i$, and the numbers a_i, β_i belong in the decomposition associated with p_i to the same progression. The theorem is thus proved.

From this theorem it follows that a regular convolution is uniquely determined by a sequence $\{\pi_{p_i}\}$, of the elements of K. It is easy to see that if the sequences associated with two convolutions A and B differ only by their order, then the convolution rings R_A and R_B are isomorphic. Indeed, if $A \sim \{\pi_{p_i}\}$, $B \sim \{\pi'_{p_i}\}$, and $\pi_{p_i} = \pi'_{p_{f(i)}}$ (where $f(i)$ is a permutation of the set $(1, 2, \ldots)$), and we define a transformation s of R_A onto R_B by

$$sg\left(\prod p_i^{a_i}\right) = g\left(\prod p_{f(i)}^{a_i}\right),$$

then s will give the desired isomorphism.

The following problem can be posed:

P 410. Is it true that if the rings R_A and R_B are isomorphic, then the sequences $\{\pi_{p_i}\}$ and $\{\pi'_{p_i}\}$ differ only by their ordering?

We are unable to answer this question. It should be remarked, that in the special case when A is the Dirichlet convolution, and $R_A \approx R_B$, B is also the Dirichlet convolution. This follows from the well-known fact that the ring R_A has no zero-divisors, for each other convolution ring must have zero-divisors (if $d \notin A_n$, then $e_d * e_{n/d} = 0$).

Let us remark that if $\{0, K_1^{(i)}, 2K_1^{(i)}, \ldots\}, \ldots \{0, K_j^{(i)}, 2K_j^{(i)}, \ldots\}, \ldots$ are the progressions belonging to the decomposition π_{p_i}, then the numbers $p_i^{K_j^{(i)}}$ are primitive numbers. Consequently we infer that if in a convolution A every primitive number is prime, then every decomposition consists of one progression: $0, 1, 2, \ldots$, and so A is a Dirichlet convolution. Similarly if in a convolution A every prime power is primitive, then every decomposition consists of two-element progressions: $0, 1; 0, 2; \ldots$, and so A must be the unitary convolution.

We give now an example which shows that, in general, the set of all primitive numbers does not determine the convolution uniquely.

Let the convolution A be defined by the sequence $\{\pi_{p_i}\}$ of decompositions, where π_2 consists of the progressions $0, 3, 6, 9, 12; 0, 4, 8; 0, 1; 0, 2; 0, 5; \ldots$ (the remaining progressions are of the form $0, k$), and the other π_{p_i} consists of 2-element progressions. Let the convolution B be defined by the sequence $\{\pi'_{p_i}\}$, where π'_2 consists of the progressions: $0, 3, 6, 9; 0, 4, 8, 12; 0, 1; \ldots$ (the remaining progressions are of the form $0, k$), and other π'_{p_i} coincide with π_{p_i}.

The primitive numbers in A and B are thus the same, but the convolutions are obviously different.

4. Now we shall prove two theorems generalizing the results of Cohen [2]. First let us define for all prime powers p^k the type of p^k as the least number $t \neq 0$ such that p^t belongs to A_{p^k}. The type of p^k shall be denoted by $\tau(p^k)$. For all primitive numbers p^k we define the rank of p^k as the greatest number r (if there exists one), such that p^k belongs to A_{p^r}. If such a number does not exist, we shall say that p^k is of infinite rank. We shall denote the rank of p^k by $r(p^k)$.

THEOREM III. *Suppose that in a regular convolution A, for all primitive numbers p^k, $r(p^k) \leqslant M$. If $f = g * h$, where $h(n) = n$, and $g(n)$ is bounded, then*

$$\sum_{n\leqslant x} f(n) = \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{g(d)\varphi(d)}{d^3}\Delta(d) + O(x\log^{2M}x)$$

for $x \geqslant 2$, where

$$\Delta(d) = \prod_{p_i|d}\frac{p_i^{\tau_i} - p_i^{a_i - r_i\tau_i}}{p_i^{\tau_i}-1} \quad \textit{for} \quad d = \prod p_i^{a_i},\ \tau_i = \tau(p_i^{a_i}),\ r_i = r(p_i^{\tau_i}).$$

Proof. Let U_m be the set of all unitary divisors of the number m, $T(x, d) = \sum_{\substack{m\leqslant x\\ d\in A_m}} m$, $T_u(x, d) = \sum_{\substack{m\leqslant x\\ d\in U_m}} m$.

Let us first observe that if $\prod_{i=1}^{k} p_i^{a_i}\in A_m$, then by Theorem 1, with suitable $\sigma_1, \ldots, \sigma_k$ $(\sigma_i \leqslant r_i - a_i/\tau_i)$

$$p_i^{a_i+\sigma_i\tau_i}\in U_m \quad (i = 1, \ldots, k),$$

and conversely; hence

$$T(x, d) = \sum_{0\leqslant\sigma_1\leqslant r_1 - a_1/\tau_1}\cdots\sum_{0\leqslant\sigma_k\leqslant r_k - a_k/\tau_k} T_u(x, p_1^{a_1+\sigma_1\tau_1}\ldots p_k^{a_k+\sigma_k\tau_k}).$$

But

$$T_u(x, d) = \sum_{\substack{m\leqslant x\\ (d, m/d)=1}} m = d\sum_{\substack{l\leqslant x/d\\ (l,d)=1}} l = \frac{x^2}{2}\cdot\frac{\varphi(d)}{d^2} + O\big(x\vartheta(d)\big)$$

(by [2], Lemma 4.1), where $\vartheta(d) = \sum_{l|d}\mu^2(l) = 2^k$, and so

$$T(x, d) = \sum_{\sigma_1}\cdots\sum_{\sigma_k}\left\{\frac{x^2(1-1/p_1)\ldots(1-1/p_k)}{2p_1^{a_1+\sigma_1\tau_1}\ldots p_k^{a_k+\sigma_k\tau_k}} + O\big(x\vartheta(d)\big)\right\}$$

$$= \frac{x^2\varphi(d)}{2d^2}\sum_{\sigma_1}\cdots\sum_{\sigma_k}\frac{1}{p_1^{\sigma_1\tau_1}\ldots p_k^{\sigma_k\tau_k}} + O\Big(x\vartheta(d)\sum_{\sigma_1}\cdots\sum_{\sigma_k}1\Big)$$

$$= \frac{x^2\varphi(d)}{2d^2}\Delta(d) + O\big(x\vartheta(d)M^k\big) = \frac{x^2\varphi(d)}{2d^2}\Delta(d) + O\big(x\vartheta(d)^{\lambda}\big),$$

where $\lambda = 1 + \log M/\log 2$.

By interchanging the order of summation, we obtain

$$\sum_{n\leqslant x} f(n) = \sum_{d\leqslant x}\frac{g(d)}{d}T(x, d) = \sum_{d\leqslant x}\frac{g(d)}{d}\left\{\frac{x^2\varphi(d)\Delta(d)}{2d^2} + O\big(x\vartheta^{\lambda}(d)\big)\right\}$$

$$= \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{g(d)\varphi(d)\Delta(d)}{d^3} + O\left(x^2\sum_{d>x}\frac{g(d)\varphi(d)\Delta(d)}{d^3}\right) + O\left(x\sum_{d\leqslant x}\frac{\vartheta^{\lambda}(d)}{d}\right).$$

The resulting series is convergent, for

$$\Delta(d) \leqslant \prod_{p_i|d}\frac{p_i^{\tau_i}-1+1}{p_i^{\tau_i}-1} = \prod_{p_i|d}\left(1+\frac{1}{p_i^{\tau_i}-1}\right) \leqslant \prod_{p_i|d}\left(1+\frac{1}{p_i-1}\right) = \frac{d}{\varphi(d)}.$$

For the same reason the second summand is $O(x)$. Now remark that $\vartheta(n) \leqslant d(n)$, where $d(n)$ is the number of divisors of the number n; hence by summation by parts and in view of the fact that

$$\sum_{n\leqslant x} d^r(n) = O(x\log^{2^r-1}x)$$

(see e. g. [6]) we obtain the estimation of the third summand which was required. The theorem is thus proved. In the case $M = 1$ this is the theorem 4.1 in [2]. Our method does not work if the $r(p^a)$ are not uniformly bounded.

THEOREM IV. *If the convolution is regular, $f = g * h$, where $h(n) = \mu^2(n)n$, and $g(n) = o(n^{\frac{1}{2}-\varepsilon})$ with some positive ε, then*

$$\sum_{n\leqslant x} f(n) = \frac{3}{\pi^2}x^2\sum_{d=1}^{\infty}\frac{g(d)\nabla(d)}{d^2} + O(x^{3/2}),$$

where

$$\nabla(d) = \prod_{\tau(p_i^{a_i})>1}\frac{p_i}{p_i+1}\cdot\prod_{\substack{\tau(p_i^{a_i})=1\\ r(p_i)=a_i}}\frac{p_i}{p_i+1}$$

for $d = p_1^{a_1}\ldots p_k^{a_k}$.

Proof. Evidently

$$\sum_{n\leqslant x} f(n) = \sum_{n\leqslant x}\sum_{d\in A_n} g(d)\mu^2(n/d)n/d = \sum_{d\leqslant x}\frac{g(d)}{d}\sum_{\substack{n\leqslant x\\ n/d\ \text{square-free}\\ d\in A_n}} n.$$

Let
$$F(x,d)=\sum_{\substack{n\leqslant x\\ n/d\ \text{square-free}\\ d\in A_n}} n \quad\text{and}\quad d=\prod_{i=1}^{k}p_i^{a_i}.$$

If $d\in A_n$, and n/d is square-free, then $n=dp_1^{\sigma_1}\dots p_k^{\sigma_k}\cdot Q$, where $(d,Q)=1$, Q is square-free, and σ_i can assume the values 0,1 if $\tau(p_i^{a_i})=1$, and $r(p_i)>a_i$; in the opposite case it can assume the value 0 only. Hence
$$F(x,d)=\sum_{\sigma_1,\dots,\sigma_k}{}'\sum n,$$
where the dash indicates that σ_i assumes the above mentioned values, the inner sum ranges over such n's of the interval $[1,x]$, for which $dp_1^{\sigma_1}\dots$ $\dots p_k^{\sigma_k}$ belongs to U_n, and n/d is square-free. Subsequently (here the double dash indicates the summation over such $n\leqslant x$, that $(d,n/dp_1^{\sigma_1}\dots p_k^{\sigma_k})=1$)
$$F(x,d)=\sum_{\sigma_1,\dots,\sigma_k}{}'\sum_{n\leqslant x}{}''\mu^2(n/dp_1^{\sigma_1}\dots p_k^{\sigma_k})n$$
$$=\sum_{\sigma_1,\dots,\sigma_k}{}'dp_1^{\sigma_1}\dots p_k^{\sigma_k}\sum_{n\leqslant x}{}''\mu^2(n/dp_1^{\sigma_1}\dots p_k^{\sigma_k})n/dp_1^{\sigma_1}\dots p_k^{\sigma_k}$$
$$=d\sum_{\sigma_1,\dots,\sigma_k}{}'Q_d'(x/dp_1^{\sigma_1}\dots p_k^{\sigma_k})p_1^{\sigma_1}\dots p_k^{\sigma_k},$$
where by $Q_d'(t)$ we denote, following [2], the sum $\sum_{\substack{m\leqslant t\\ (m,d)=1}}\mu^2(m)m$.

In view of [2] (lemma 5.3) we have
$$Q_d'(t)=\left(\frac{3}{\pi^2}\prod_{p|d}\frac{p}{p+1}\right)t^2+O\left(t^{3/2}\vartheta(d)\right);$$
hence (with the notation $S(d)=\frac{3}{\pi^2}\prod_{p|d}\frac{p}{p+1}$)
$$F(x,d)=d\sum_{\sigma_1,\dots,\sigma_k}{}'\left\{S(d)\frac{x^2}{d^2p_1^{2\sigma_1}\dots p_k^{2\sigma_k}}+O\left(\frac{x^{3/2}}{d^{3/2}}\cdot\frac{\vartheta(d)}{(p_1^{\sigma_1}\dots p_k^{\sigma_k})^{3/2}}\right)\right\}p_1^{\sigma_1}\dots p_k^{\sigma_k}$$
$$=\frac{S(d)}{d}x^2\sum_{\sigma_1,\dots,\sigma_k}{}'\frac{1}{p_1^{\sigma_1}\dots p_k^{\sigma_k}}+O\left(\frac{x^{3/2}}{\sqrt{d}}\vartheta(d)\sum_{\sigma_1,\dots,\sigma_k}{}'\frac{1}{\sqrt{p_1^{\sigma_1}\dots p_k^{\sigma_k}}}\right)$$
$$=\frac{S(d)}{d}x^2\prod_{\substack{p_i^{a_i}\in U_d\\ \tau(p_i^{a_i})=1\\ r(p_i)>a_i}}\left(1+\frac{1}{p_i}\right)+O\left(\frac{x^{3/2}}{\sqrt{d}}\vartheta(d)\prod_{\substack{p_i^{a_i}\in U_d\\ \tau(p_i^{a_i})=1\\ r(p_i)>a_i}}\left(1+\frac{1}{\sqrt{p_i}}\right)\right)$$
$$=\frac{3}{\pi^2}\cdot\frac{\nabla(d)}{d}x^2+O\left(\frac{x^{3/2}}{\sqrt{d}}\vartheta(d)\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right)\right).$$

Consequently
$$\sum_{n\leqslant x}f(n)=\sum_{d\leqslant x}\frac{g(d)}{d}F(x,d)$$
$$=\frac{3}{\pi^2}x^2\sum_{d=1}^{\infty}\frac{g(d)\nabla(d)}{d^2}+O\left(x^2\sum_{d>x}\frac{g(d)\nabla(d)}{d^2}\right)+O\left(x^{3/2}\sum_{d\leqslant x}\frac{g(d)}{d^{3/2}}\vartheta(d)\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right)\right).$$

The series is convergent, because $\nabla(d)g(d)=O(d^{1/2-\varepsilon})$, and the second summand is $O(x^{3/2-\varepsilon})$.

Observe now, that
$$\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right)\leqslant(1+1/\sqrt{2})^k,$$
where k is the number of different prime divisors of the number d, and $\vartheta(d)=2^k$; hence
$$x^{3/2}\sum_{d\leqslant x}\frac{g(d)\vartheta(d)\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right)}{d^{3/2}}=O\left(x^{3/2}\sum_{d\leqslant x}\frac{\vartheta(d)\prod_{p|d}\left(1+\frac{1}{\sqrt{p}}\right)}{d^{1+\varepsilon}}\right)$$
$$=O\left(x^{3/2}\sum_{d\leqslant x}\frac{\vartheta(d)^{1+\log(1+1/\sqrt{2})\log^{-1}2}}{d^{1+\varepsilon}}\right)=O(x^{3/2})$$
as $\vartheta(d)=o(d^\lambda)$ for every positive λ. This gives the required evaluation of the third summand, and the theorem is proved.

COROLLARY. *By putting in the above proved theorems $g(n)=1$, we obtain*

$$(\alpha)\qquad \sum_{n\leqslant x}\sigma_A(n)=\frac{x^2}{2}\sum_{n=1}^{\infty}\frac{\varphi(n)\Delta(n)}{n^3}+O(x\log^{2M}x)$$

in the case when $r(p^\tau)\leqslant M$ ($\sigma_A(n)$ is the sum of the numbers appearing in A_n);

$$(\beta)\qquad \sum_{n\leqslant x}\sigma_A'(n)=\frac{x^2}{2}\prod_{p}\left(1-\frac{1}{p+1}\cdot\frac{1}{p^{2r(p)}}\right)+O(x^{3/2})$$

($\sigma_A'(n)$ is the sum of all square-free numbers appearing in A_n).

The equality (β) follows in a simple way from theorem IV with the use of Euler products.

5. Let us assume, that A is a regular convolution. In the ring R_A one can distinguish a subring B_A, consisting of the functions f with finite norm: $\|f\| = \sum_{n=1}^{\infty} |f(n)|$. The ring B_A can be dealt with as an algebra upon the complex field, moreover B_A is a Banach algebra, since

$$\|f*g\| = \sum_{n=1}^{\infty}\Big|\sum_{d\in A_n} f(d)g(n/d)\Big| \leqslant \sum_{n=1}^{\infty}\sum_{d\in A_n}|f(d)|\,|g(n/d)|$$

$$\leqslant \sum_{n=1}^{\infty}\sum_{d|n}|f(d)g(n/d)| = \sum_{n=1}^{\infty}\sum_{uv=n}|f(u)|\cdot|g(v)| = \sum_{u=1}^{\infty}\sum_{v=1}^{\infty}|f(u)|\cdot|g(v)| = \|f\|\cdot\|g\|.$$

In the case of Dirichlet convolution, B_A is evidently isomorphic with the l_1-algebra of the multiplicative semigroup of positive integers. In the general case B_A happens to be in some sense very "near" the l_1-algebra of a suitable semigroup. Indeed, let us define a multiplication in the set of all non-negative integers by:

$$0\circ m = m\circ 0 = 0,$$

$$m\circ n = \begin{cases} 0, & m\notin A_{mn}, \\ mn, & m\in A_{mn}. \end{cases}$$

This multiplication defines a semigroup G. Let us define a "near-to-convolution" multiplication in the set of all functions on G which vanish at zero and have finite norm $\sum_{n=1}^{\infty}|f(n)|$ as follows:

$$(f\times g)(0) = 0,$$

$$(f\times g)(n) = \sum_{u\circ v=n} f(u)g(v) \qquad (n\neq 0);$$

the obtained normed ring (with usual addition) is isomorphic with B_A.

Now we shall find the maximal ideals in B_A or, which means the same, we shall find the non-trivial homomorphisms of B_A into the field of complex numbers.

Let P be the set of all primitive numbers of infinite rank (from theorem II and the obvious fact, that two infinite arithmetic progressions containing zero must have common elements it follows that every two numbers from the set P are relatively prime).

Every natural number $n\neq 1$ can be uniquely written in the form

$$n = \prod_i (q_i^{\tau_i})^{a_i},$$

where the $q_i^{\tau_i}$ are primitive numbers belonging to the set A_n. Let χ be any homomorphism of B_A into the complex field Z. If $q^\tau\notin P$, then, as for some r, $q^\tau\notin A_{q^{r\tau}}$, e_j (where $j = q^\tau$) is nilpotent, and so $\chi(e_j) = 0$. For every n, $\chi(n) = \prod_i \big(\chi(e_{q_i}^{\tau_i})\big)^{a_i}$ and we see that if not all of the $q_i^{\tau_i}$ belong to P, then $\chi(n) = 0$. As every homomorphism $B_A\to Z$ is continuous, it is determined by the values assumed for e_{j_i}, where $j_i\in P$. Let $\lambda_i = \chi(e_{j_i})$ (evidently $|\lambda_i|\leqslant 1$). Obviously $\chi(e_1) = 1$, and so every homomorphism must have the form

$$\chi(f) = f(1) + \sum f(k)\prod_i \lambda_i^{a_i}, \tag{4}$$

where the summation runs over all k of the form $\prod_i (p_i^{\tau_i})^{a_i}$, where $p_i^{\tau_i}$ belong to P.

Conversely, the mapping defined by (4) with $|\lambda_i|\leqslant 1$ defines obviously a homomorphism: $B_A\to Z$. Hence we have proved

THEOREM V. *If M is a maximal ideal in B_A, then there exists a sequence $\{\lambda_1, \lambda_2, \ldots\}$ (which is finite and has s elements if P has s elements, and is infinite if P is) of complex numbers satisfying $|\lambda_i|\leqslant 1$ $(i = 1, 2, \ldots)$, such that*

$$M = \Big\{f\in B_A : f(1) + \sum_{k=\prod_i (p_i^{\tau_i})^{a_i}} f(k)\prod_i \lambda_i^{a_i} = 0\Big\},$$

where the $p_i^{\tau_i}$ belong to the set P.

Conversely, every such sequence defines a maximal ideal.

The following theorem shows that the cardinal number of the set P is the single invariant of homeomorphisms of the space $\mathfrak{M}(B_A)$ of the maximal ideals of B_A.

THEOREM VI. *If s is the cardinal number of the set P, then the space $\mathfrak{M}(B_A)$ is homeomorphic with K^s, where K is the set $\{z: |z|\leqslant 1\}$ in the complex plane.*

Proof. From theorem V it follows that the sets of elements of $\mathfrak{M}(B_A)$ and K^s can be identified. Now we remark that with the notation $\tilde{f}(M)$ for the Gelfand transform of f,

$$\tilde{f}(M) = \tilde{f}(\lambda_1, \lambda_2, \ldots) = \sum_{\substack{k=\prod_{i=1}^{r}(p_i^{\tau_i})^{a_i} \\ p_i^{\tau_i}\in P}} f(k)\lambda_1^{a_1}\ldots\lambda_r^{a_r};$$

hence the functions $\tilde{f}(M)$ are continuous in K^s and in view of the compactness of K^s we obtain the homeomorphism of $\mathfrak{M}(B_A)$ and K^s (see e. g. [4], th. 1′, p. 39).

COROLLARY. *In the case of the unitary convolution, the set P is void; hence $s = 0$, and so there is only one maximal ideal, consisting of all functions vanishing for $n = 1$.*

Consequently we infer that every function $f(n)$ non-vanishing for $n = 1$ has an inverse in the unitary ring B_U, or, in other words, if f has an inverse g in R_U, and the series $\sum_{n=1}^{\infty} |f(n)|$ is convergent, then the series $\sum_{n=1}^{\infty} |g(n)|$ is also convergent.

From the theorem 5.8 in [5] we infer that in the Dirichlet case the algebra B_A is semisimple. From the remark, that every other algebra B_A has nilpotent elements it follows that the semisimplicity of B_A is a characteristic property of the Dirichlet convolution.

REFERENCES

[1] E. T. Bell, *Factorability of numerical functions*, Bulletin of the American Mathematical Society 37 (1931), p. 251-253.

[2] E. Cohen, *Arithmetical functions associated with the unitary divisors of an integer*, Mathematische Zeitschrift 74 (1960), p. 66-80.

[3] — *Unitary products of arithmetical functions*, Acta Arithmetica 7 (1961), p. 29-38.

[4] И. М. Гельфанд, Д. А. Райков и Г. Е. Шилов, *Коммутативные нормированные кольца*, Москва 1960.

[5] E. Hewitt and H. S. Zuckerman, *The l_1-algebra of a commutative semi-group*, Transactions of the American Mathematical Society 83 (1956), p. 70-97.

[6] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proceedings of the London Mathematical Society, (2), 21 (1922), p. 235-255.

Reçu par la Rédaction le 5. 1. 1962

COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

SUR UN PROBLÈME DE K. URBANIK CONCERNANT LA DIMENSION DE HAUSDORFF

PAR

J.-L. LIBOUBAN ET N. RIEU (MONTPELLIER)

Urbanik a posé le problème suivant (1):

Le semi-groupe additif engendré par un ensemble parfait situé sur la demi-droite $(0, \infty)$ et ayant une dimension de Hausdorff positive dans tout voisinage de 0 contient-il nécessairement toute la demi-droite?

La réponse est négative. J.-P. Kahane nous a indiqué le principe de la construction d'un exemple contraire et proposé de réaliser cette idée. *L'ensemble E que nous allons exhiber a pour dimension de Hausdorff le nombre 1 dans tout voisinage de l'origine et le semi-groupe additif qu'il engendre ne contient dans $[0, 1]$ qu'un ensemble de points de mesure de Lebesgue nulle.*

1. Construction de E et propriétés immédiates. E sera un ensemble linéaire formé par la réunion d'ensembles disjoints dont les segments supports ont pour extrémités gauches les points 2^{-j} et des longueurs très rapidement décroissantes

$$E = \{0\} \cup \Big(\bigcup_{j=1}^{\infty} E_j\Big),$$

$$E_j = \Big\{2^{-j} + \sum_{k=0}^{\infty} \varepsilon_k a_{j+k}, \quad \text{où} \quad \varepsilon_k = 0 \text{ ou } 1, \text{ ou} \ldots, \text{ ou } 2^k\Big\}$$

où les accolades désignent l'ensemble des points de la forme écrite, et où $\{a_n\}$ est une suite rapidement décroissante de nombres réels positifs qu'on déterminera.

Les segments supports de E_j et E_{j-1} $(j = 2, 3, \ldots)$ sont disjoints si et seulement si

$$\sum_{k=0}^{\infty} 2^k a_{j+k} < 2^{-j}. \tag{1}$$

(1) K. Urbanik, **P 322**, Colloquium Mathematicum 8 (1961), p. 139.