数理解析研究所講究録
第 84 巻 1970 年 112-136

加法数論における
一つの確率論的方法について

信州大 理　　鹿野　　健

§1：　　問題の起りと諸定理.

まず，以下で用いる記号の定義から。

(def. 1)　自然数全体を $\mathcal{N}$ で表わし，$\mathcal{A} \subset \mathcal{N}$ とする。

(def. 2)　$n \in \mathcal{N}$ を

$$n = a + a'$$

$$(a < a', \quad a, a' \in \mathcal{A})$$

と表わす「表わし方の個数」を $r_n(\mathcal{A})$ と書く。

(def. 3)　$n \in \mathcal{N}$ を

$$n = a + a'$$

$$(a \leq a', \quad a, a' \in \mathcal{A})$$

と表わす「表わし方の個数」を $r_n'(\mathcal{A})$ と書く。

すると，明かに次の関係がある。

$$r_n'(\mathcal{A}) = \begin{cases} r_n(\mathcal{A}) + 1, & \cdots\cdots \frac{n}{2} \in \mathcal{A}. \\ r_n(\mathcal{A}), & \cdots\cdots \frac{n}{2} \notin \mathcal{A}. \end{cases}$$

(def. 4)　十分大きいすべての $n \in \mathcal{N}$ に対して

$r_n'(\mathcal{A}) > 0$ となるならば，$\mathcal{A}$ を次数2の

「漸近基」（asymptotic basis of order 2）とよぶ。

(def. 5)　$\mathcal{A}$ が $B_2[g]$ のクラスに属する，あるいは $B_2[g]$

数列である，というのは，すべての $n \in \mathcal{N}$ に対して

$$r_n'(\mathcal{A}) \leqq g$$

となることをいう。

(def. 6)　上の定義で，特に $g = 1$ のとき，即ち $B_2[1]$ 数

列を簡単のために B_2 数列とよぶことにする。

def. 3 と def. 5 より，

$r_n(\mathcal{A}) \leqq g$ ならば $\mathcal{A} \in B_2[g+1]$

であることは明かであるが，以下で用いる確率論的方法に

おいては $r_n'(\mathcal{A})$ よりも $r_n(\mathcal{A})$ の方が扱い易いので，

以下では $r_n'(\mathcal{A})$ は登場して来ないが，我々の証明する

結果（→ 定理B）には何の影響も与えない。

S. Sidon（Szidon とも書く）は Math. Ann.

106 (1932) 536～539 の論文

"Ein Satz über trigonometrische Polynome und

seine Anwendungen in der Theorie der Fourier-

Reihen."

なる論文において，我々の記号を用いて表現すれば，結局次のような2つの問題を提起している。

[Sidon の第1問題]

$\forall \varepsilon > 0$ に対して，

$$\lim_{n\to\infty} \frac{r_n(A)}{n^{\varepsilon}} = 0$$

となるような 次数2の漸近基 は存在するか？

[Sidon の第2問題]

$A \in B_2[g]$, $A = \{a_j\}$, ($a_j \in N$: $j = 1, 2, 3, \ldots$)

ならば， a_j は j の函数としてどういう大きさをもつか？

第1問題は P. Erdös によって，

" Problems and results in additive number theory."

(Colloque sur la théorie des nombres: Bruxelles , 1956)

において次の形で解決された。

[定理 A] (P. Erdös)

$$\log n \ll r_n(\mathcal{A}) \ll \log n$$

であるような次数2の漸近基 $\mathcal{A}$ が存在する。

一方，第2問題に対しては未だに十分な解答が得られていない。　g_2 数列に限れば，現在得られている結果は次の様なものである。

(a)　任意の $\mathcal{A}=\{a_j\} \in B_2$ に対して，

i)　$\displaystyle\limsup_{j\to\infty} \frac{a_j}{j^2} = +\infty$　(Erdös-Turán : 1941)

ii)　$\displaystyle\limsup_{j\to\infty} \frac{a_j}{j^2\log j} > 0$　(Erdös : 1955 頃)

明かに ii) より i) が従う。

(b)　次のような $\mathcal{A}=\{a_j\} \in B_2$ が存在する。

i)　$\displaystyle\liminf_{j\to\infty} \frac{a_j}{j^2} < +\infty$　(Erdös : 1955 頃)

あるいは

ii)　$a_j \ll j^3$　(Mian - Chowla : 1944)

[Erdös の予想]

$\forall \varepsilon > 0$ に対して，$a_j \ll j^{2+\varepsilon}$

であるような $\mathcal{A} \in B_2$ が存在する。

[Erdös - Turán の予想]

$$\mathcal{A} = \{a_j\}, \quad a_j \ll j^2$$

ならば，
$$\limsup_{n\to\infty} r_n(\mathcal{A}) = +\infty \quad ,$$

あるいはこれよりも弱く．

$\mathcal{A}$ が次数 2 の漸近基ならば．

$$\limsup_{n\to\infty} r_n(\mathcal{A}) = +\infty \quad .$$

以上はいずれも未解決であるが，Erdös の予想に関して，Erdös と Rényi は次の結果を得た。

(Erdös - Rényi : *Additive properties of random sequences of positive integers*. Acta Arith. 6 (1960) 83〜110)

[定理 B] (Erdös - Rényi)

$\forall \varepsilon > 0$ に対応して，$g = g(\varepsilon)$ と $B_2[g]$ 数列 $\mathcal{A}$ が存在して，

$$a_j \ll j^{2+\varepsilon} \quad .$$

(def. 7) 与えられた数列 $\mathcal{A}$ に対して，数列 $\mathcal{B}$ が $\mathcal{A}$ の「補数列」(complementary sequence) であるとは，十分大きいすべての $n \in \mathcal{N}$ が

$$n = a + b \qquad (a \in \mathcal{A},\ b \in \mathcal{B})$$

と表わされることを言う。

(def. 8) $\mathcal{A}$ の要素で $n \in \mathcal{N}$ をこえないものの個数を「計数」(counting number) とよび、$A(n)$ で表わす。def. 7 における $\mathcal{B}$ に対しても同様に $B(n)$ を定義する。

[定理C] (P. Erdős : Proc. Am. Math. Soc. (1954) 847〜853)

$\mathcal{P}$ でもって素数全体を表わすことにすると、$\mathcal{P}$ の補数列 $\mathcal{B}$ で、

$$B(n) \sim c(\log n)^2,$$

となるものが存在する。

以上の定理A〜Cを証明するのが目的であるが、それらは主としてErdősによって考えられ、Erdős−Rényi の前出の論文において発表された、一つの確率論的な方法で統一的に証明できるのである。ここでは、それを更に整理して formulation を完全にした、Halberstam と Roth の著書 "Sequences" vol. I (Oxford: 1966) の第Ⅲ章に従って述べることにする。

§2：　確率論からの準備.

我々は Kolmogorov によって建てられた測度論的確率論の基本定理の上に立つが，定理A～C の証明にはそれほど多くの定理を確率論から要する訳ではない。確率論の構成が目的ではないから，以下ではすべての定理に証明を与えることはしないで，必要なものを並べる，と言う程度にする。測度論的確率論における基本的な用語の定義や概念を仮定する。

[定理 1]　(Wiener-Kolmogorov-Kakutani)

$(X_j, \mathfrak{S}_j, \mu)$ を確率空間の列とし，X_j の直積を $\bigtimes_{j=1}^{\infty} X_j$ で表わし，

$$X = \bigtimes_{j=1}^{\infty} X_j$$

とする。そして，$\mathfrak{S}$ を $\{\mathfrak{S}_j\}$ に関する任意の矩形集合を含むような最小の σ-代数であるような，X の部分集合体とすると，この $\mathfrak{S}$ 上に定義される，次のような測度 μ が unique に定まる。即ち，任意の矩形集合 $E = \bigtimes_{j=1}^{\infty} E_j$ に対して

$$\mu(E) = \prod_{j=1}^{\infty} \mu_j(E_j)$$

となるものである。ここに，$E_j \in \mathfrak{S}_j$ $(j \geqq 1)$，$E_j = X_j$ $(j \geqq j_0)$。

(def. 9)　自然数から成る数列を ω とし，そのような
すべての ω から成る「空間」を Ω とする。
すると，定理1の系として次の定理を得る。

[定理2]

$$\{\alpha_j\}\ ;\quad 0 \leq \alpha_j \leq 1 \quad (j = 1, 2, \ldots\ldots)$$

なる実数列に対応して，次のような性質をもつ確率空間
$(\Omega, \mathfrak{F}, \mu)$ が存在する。

i) $\forall n \in N$ に対して，事象

$$B_n = \{\omega : n \in \omega\}$$

は可測で，$\mu(B_n) = \alpha_n$.

ii) 事象 $B_1, B_2, \ldots\ldots$ は独立。

(証明)　Y を，$Y = \{y^{(0)}, y^{(1)}\}$ なる空間とする。

次に，
$$x_j = \begin{cases} y^{(1)} & \cdots\cdots\ j \in \omega \\ y^{(0)} & \cdots\cdots\ j \notin \omega \end{cases}$$

とし，$x = \{x_j\}$ なるすべての数列から成る空間を X
とすれば，X は明かに

$$X = \mathop{\times}_{j=1}^{\infty} X_j\ ,\qquad X_j = Y\ \ (j \geq 1)$$

で与えられる。そして，X_j の4つの部分集合から
成る σ-代数を $\mathfrak{F}_j$ とし，$\mathfrak{F}_j$ 上の確率測度で，
$y^{(1)}$ だけからなるような X_j の部分集合の上で α_j なる
値をとるものを μ_j とする。

このようにして定められた確率空間の列 $(X_j, \mathfrak{S}_j, \mu_j)$ に対して 定理1 を適用すると，X と Ω の間に1対1対応が成立することに注意すれば，$(\Omega, \mathfrak{S}, \mu)$ なる確率空間が存在して，i)，ii) が成立すること明かである。

(def. 10) 確率変数 f の期待値（一次モーメント）を

$$M(f) \overset{\text{df.}}{=} \int_\Omega f\, d\mu \quad ,$$

分散（variance）を

$$D^2(f) \overset{\text{df.}}{=} M(\{f - M(f)\}^2)$$

と書く。

[定理3] $\{g_i\}$ を独立な確率変数とし，$M(g_j)=0$ $(j \geqq 1)$ とする。もし

$$\sum_{j=1}^{\infty} D^2(g_j) < +\infty$$

ならば，確率 1 で

$$\sum_{j=1}^{\infty} g_j(x) < +\infty \quad .$$

[定理4] $\{f_i\}$ を独立な確率変数の列とする。

$$s_i = \sum_{j=1}^{i} f_j \qquad (i \geqq 1)$$

とし，

$$M(f_j) > 0 \quad , \quad (j \geqq 1)$$

$$\lim_{i\to\infty} M(s_i) = +\infty ,$$

かつ $$\sum_{i=1}^{\infty} \frac{D^2(f_i)}{\{M(s_i)\}^2} < +\infty ,$$

とすると，確率 1 で

$$s_i(x) \sim M(s_i) \qquad (i \to \infty)$$

証明）

$$g_i(x) = \frac{f_i(x) - M(f_i)}{M(s_i)} \qquad (i \geqq 1)$$

とすると，

$$M(g_i) = M\left(\frac{f_i(x)}{M(s_i)} - \frac{M(f_i)}{M(s_i)}\right) = \frac{M(f_i)}{M(s_i)} - \frac{M(f_i)}{M(s_i)}$$

$$= 0$$

また，
$$D^2(g_i) = M(g_i^2) - \{M(g_i)\}^2 = M(g_i^2)$$
$$= M\left(\left\{\frac{f_i(x) - M(f_i)}{M(s_i)}\right\}^2\right)$$
$$= \frac{M(\{f_i - M(f_i)\}^2)}{M(s_i)^2} = \frac{D^2(f_i)}{M(s_i)^2} .$$
$$\therefore \sum_{i=1}^{\infty} \frac{D^2(f_i)}{M(s_i)^2} = \sum_{i=1}^{\infty} D^2(g_i) < +\infty .$$

そして明かに $\{g_i\}$ は独立であるから，この $\{g_i\}$ は定理 3 の（g_i の）条件を満足する。 従って，確率 1 で

$$\sum_{i=1}^{\infty} \frac{\{f_i(x) - M(f_i)\}}{M(s_i)} < +\infty$$

となる。

そこで，次の良く知られた lemma を用いる。

（Lemma） $\sum_{j=1}^{\infty} a_j$ が収束するとき，$\{m_j\}$ $(j \geqq 1)$ を任意の単調に増大して $+\infty$ に発散する正数列とすると，

$$\lim_{i\to\infty}\frac{1}{m_i}\sum_{j=1}^{i} a_j m_j = 0 .$$

この Lemmaにおいて, $a_j = \dfrac{f_j(x) - M(f_j)}{M(S_j)}$,

$m_j = M(S_j)$,

と置けば, Lemma より

$$\lim_{i\to\infty}\frac{1}{M(S_i)}\sum_{j=1}^{i}\{f_j(x) - M(f_j)\} = 0 .$$

所が,

$$\frac{1}{M(S_i)}\sum_{j=1}^{i}\{f_j(x) - M(f_j)\} = \frac{\sum_{j=1}^{i} f_j(x) - \sum_{j=1}^{i} M(f_j)}{M(S_i)}$$

$$= \frac{\sum_{j=1}^{i} f_j(x) - M(\sum_{j=1}^{i} f_j)}{M(S_i)} = \frac{S_i - M(S_i)}{M(S_i)} = \frac{S_i}{M(S_i)} - 1$$

であるから, 証明すべき.

a.s. $\dfrac{S_i}{M(S_i)} \longrightarrow 1$ を得た。

[定理 5] (Borel - Cantelli)

$\{E_j\}$ $(j \geqq 1)$ を可測事象の列とする。

もし $\sum_{j=1}^{\infty}\mu(E_j) < +\infty$

ならば, 確率 1 で, 高々有限個の E_j の事象が起る。

§3： 定理A，B，C の証明のための準備．

以下では定理２に現われた確率空間（$\Omega, \mathfrak{S}, \mu$）を取る。

(def. 11) $\rho_n(\omega)$ を事象 B_n の特性函数，即ち

$$\rho_n(\omega) = \begin{cases} 1 & \cdots\cdots n \in \omega \\ 0 & \cdots\cdots n \notin \omega \end{cases}$$

とする。

(def. 12) $s^*_n = s^*_n(\omega)$ を ω の計数，即ち，$n \in \mathcal{N}$ を越えないような ω の要素の個数とする。

以上の定義より，

$$s^*_n(\omega) = \sum_{j=1}^{n} \rho_j(\omega),$$

$$r_n(\omega) = \sum_{1 \leq j < \frac{n}{2}} \rho_j(\omega)\, \rho_{n-j}(\omega),$$

を得る。

(def. 13)
$$m^*_n \overset{df}{=} M\{s^*_n(\omega)\} = \sum_{j=1}^{n} \alpha_j,$$

$$\lambda_n \overset{df}{=} M\{r_n(\omega)\} = \sum_{1 \leq j < \frac{n}{2}} \alpha_j\, \alpha_{n-j},$$

$$\lambda'_n \overset{df}{=} \sum_{1 \leq j < \frac{n}{2}} \frac{\alpha_j\, \alpha_{n-j}}{1 - \alpha_j\, \alpha_{n-j}}.$$

$\{\alpha_j\}$ は定理２における数列である。

我々はこの $\{\alpha_j\}$ について，次の仮定を考える。

［仮定 A］ $0 < \alpha_j < 1 \quad (j \geq 1)$ であって，ある番号 j_0 から先は単調に減少して 0 に収束する。即ち，

$$\alpha_j \downarrow 0 \qquad (j \to \infty).$$

定理４において　$f_i = \rho_i$　とおくと，

$$D^2(\rho_j) = \alpha_j - \alpha_j^2$$

であることに注意すると次の lemma を得る。

（Lemma 1）　仮定Aが成立していて，

$$m_n^* \to +\infty \quad (n \to \infty)$$

$$\sum_{n=1}^{\infty} \frac{\alpha_n}{(m_n^*)^2} < +\infty$$

であるならば，確率１で

$$s_n^*(\omega) \sim m_n^* \quad (n \to \infty).$$

（注意）　上の lemma で，　n の代りに a_j　（$\omega = \{a_j\}$）を入れれば，定義から　$s_{a_j}^*(\omega) = j$　であるから，

$$j \sim m_{a_j}^*$$

を得る。　従って，m_n^* が　n の函数としてその大きさが分れば，それから a_j の（j の函数としての）大きさが分る。

（Lemma 2）　$\{\alpha_j\}$ を，仮定Aを満たす次のような数列とする。

$$\alpha_j = \alpha \frac{(\log j)^{c'}}{j^c} \quad (j \geqq j_0).$$

ここに，j_0，α，c，c' は定数で，仮定Aが成立するようなものであり，更に

$$\alpha > 0, \quad 0 < c < 1, \quad c' \geqq 0.$$

とする。

すると，$n \to \infty$ のとき，

$$\begin{cases} \lambda_n \sim \dfrac{\alpha^2}{2} \cdot \dfrac{\{\Gamma(1-c)\}^2}{\Gamma(2-2c)} (\log n)^{2c'} n^{1-2c}, \\ \\ m_n^* \sim \dfrac{\alpha}{1-c} (\log n)^{c'} n^{1-c}. \end{cases}$$

これより，特に $c'=0$ のとき，確率1で，

$$a_j \sim \left(\frac{1-c}{\alpha} j\right)^{\frac{1}{1-c}}, \qquad (j \to \infty)$$

となる。 そこで更に $\alpha = \frac{1}{2}$，$c = \frac{1}{2}$ とすれば，

$$a_j \sim j^2 \qquad (j \to \infty),$$

即ち a_j は pseudo-square である。

（証明） nは十分大で，$o(1)$ はすべてnに関するものとし，$\delta_n = \dfrac{1}{\log n}$ とする。 すると，

$$\sum_{j \leq n\delta_n} \frac{1}{\{j(n-j)\}^c} \ll \frac{1}{n^c} \sum_{j \leq n\delta_n} \frac{1}{j^c} = o(n^{1-2c}),$$

であり，$1 \leq j \leq j_0$ では，$0 < \alpha_j < 1$ であるから，

$$\alpha_j \alpha_{n-j} \ll \alpha_{n-j} \ll (\log n)^{c'} n^{-c} = o(n^{1-2c})$$

であるから，

$$\lambda_n = \alpha^2 \sum_{n\delta_n < j < \frac{n}{2}} \frac{\{(\log j)(\log(n-j))\}^{c'}}{(j(n-j))^c} + o\{(\log n)^{2c'} n^{1-2c}\}.$$

所が，$n\delta_n < j < \frac{n}{2}$ のとき

$$(\log j)(\log(n-j)) = \{1 + o(1)\}(\log n)^2$$

であるから，結局

$$\lambda_n = \alpha^2\{1+o(1)\}(\log n)^{2c'}\sum_{1\le j<\frac{n}{2}}\frac{1}{\{j(n-j)\}^c} + O\{(\log n)^{2c'} n^{1-2c}\}.$$

ここで，$\phi(t) = \{t(1-c)\}^{-c}$，$t_j = \frac{j}{n}$ とすると，

$$n^{2c-1}\sum_{1\le j<\frac{n}{2}}\frac{1}{\{j(n-j)\}^c} = \sum_{1\le j<\frac{n}{2}}\phi(t_j)\cdot(t_j - t_{j-1})$$

$$= \{1+o(1)\}\int_0^{\frac{1}{2}}\phi(t)\,dt$$

$$= \frac{1}{2}\{1+o(1)\}B(1-c,\ 1-c)$$

$$= \frac{1}{2}\{1+o(1)\}\frac{\{\Gamma(1-c)\}^2}{\Gamma(2-2c)}.$$

従って，
$$m_n^* = \sum_{j=1}^{n}\alpha\frac{(\log j)^{c'}}{j^c} + O(1)$$

$$= \{1+o(1)\}\frac{\alpha}{1-c}(\log n)^{c'} n^{1-c},$$

を得る。

q.e.d.

（注意） 上の m_n^* は明かに Lemma 1 の仮定を満たしている。

（Lemma 3） $\{\alpha_j\}$ は定理2におけるもので，

$$\alpha_j = \alpha\frac{\log j}{j} \qquad (j \geq j_0),$$

j_0，α は正の定数で，

$$0 < \alpha_j < 1 \qquad (j \geq 1)$$

となるようなものとする。このとき，$n\to\infty$ に対して，

$$m_n^* \sim \frac{\alpha}{2}(\log n)^2,$$

であり，確率1で

$$s_n^*(\omega) \sim \frac{\alpha}{2}(\log n)^2 .$$

(Lemma 4)　$n \in \mathcal{N}$，dは非負の整数とすると，

$$\mu(\{\omega ; r_n(\omega)=d\}) = \Big(\prod_{1\leq k<\frac{n}{2}} (1-\alpha_k \alpha_{n-k})\Big)\sigma_d^{(n)},$$

ここに，$\sigma_0^{(n)}=1$ で，$d \geqq 1$ のときは

$$\sigma_d^{(n)} = \sum_{1\leq k_1<k_2<\cdots<k_d<\frac{n}{2}} \prod_{j=1}^{d} \frac{\alpha_{k_j}\alpha_{n-k_j}}{1-\alpha_{k_j}\alpha_{n-k_j}} .$$

(証明)　$d=0$ のときは明かに成立する。$d \geqq 1$ のとき，

$$\mu(\{\omega ; r_n(\omega)=d\}) = \sum_{1\leq k_1<\cdots<k_d<\frac{n}{2}} \mu\{E(k_1,\ldots,k_d)\},$$

ここに，$E(k_1,\ldots,k_d)$ は，

$$\{\omega : \rho_k \rho_{n-k} = 1 \iff k \in \{k_j\} \ (j=1,2,\ldots,d)\}$$

なる事象とする。明かに

$$\mu\{E(k_1,\ldots,k_d)\} = \Big\{\prod_{j=1}^{d} \alpha_{k_j}\alpha_{n-k_j}\Big\}\Big\{\prod_{\substack{1\leq k<\frac{n}{2} \\ k\neq k_j \\ (1\leq j\leq d)}} (1-\alpha_k\alpha_{n-k})\Big\}$$

$$= \Big\{\prod_{1\leq k<\frac{n}{2}} (1-\alpha_k\alpha_{n-k})\Big\}\Big\{\prod_{j=1}^{d} \frac{\alpha_{k_j}\alpha_{n-k_j}}{1-\alpha_{k_j}\alpha_{n-k_j}}\Big\},$$

であるから証明された。

(注意)　$d \geqq \frac{n}{2}$ のときは，$\sigma_d^{(n)}$ の和は空であって，やはり Lemma 4 は成立する。

(Lemma 5)　y_j $(1 \leq j \leq N)$ を非負の整数とする。

各 $d \in \mathcal{N}$ に対応して $(d \leq N)$，

$$\sigma_d = \sum_{1\leq k_1<\cdots<k_d\leq N} y_{k_1} y_{k_2} \cdots y_{k_d} ,$$

即ち，σ_d を d 次の基本対称式とすると，

$$\sigma_d \leqq \frac{1}{d!}\sigma_1^d .$$

（証明）　明かに

$$\sigma_1 \sigma_d \geqq (d+1)\sigma_{d+1}$$

であるから，帰納法によって

$$\sigma_d \leqq \frac{1}{d!}\sigma_1^d$$

の成立することが分る。

（Lemma 6）　$n \in N$，d は非負の整数とすると，

$$\mu(\{\omega : r_n(\omega) = d\}) \leqq \frac{(\lambda_n')^d}{d!} e^{-\lambda_n} .$$

（証明）　$d \geqq \frac{n}{2}$ の場合は $r_n(\omega) = d$ なる事象は空であるから明かに成り立つ。$d < \frac{n}{2}$ のときは，Lemma 5 において $y_k = \dfrac{\alpha_k \alpha_{n-k}}{1-\alpha_k \alpha_{n-k}}$ とおけば，

$$\mu(\{\omega : r_n(\omega) = d\}) \leqq P \frac{(\lambda_n')^d}{d!} .$$

ここに，

$$P = \prod_{1 \leqq k < \frac{n}{2}} (1 - \alpha_k \alpha_{n-k}) .$$

しかし，$0 < t < 1$ のとき，不等式

$$1 - t < e^{-t}$$

が成立するから，これより $P < e^{-\lambda_n}$ となり，この lemma は証明された。

（Lemma 7）　仮定 A が成立していれば，$n \to \infty$ のとき

$$\lambda_n' \sim \lambda_n .$$

(証明)　$1 \leqq k < \frac{n}{2}$ で n が十分大きいとき，仮定より $n \to \infty$ のとき

$$\alpha_k \alpha_{n-k} \leqq \alpha_{n-k} \leqq \alpha_{[\frac{n}{2}]} = o(1)$$

であるから，これより明かに Lemma 7 の主張が成立する。

(Lemma 8)

$0 < \xi \leqq U$ ならば，

(i) $$\sum_{d \geqq U} \frac{\xi^d}{d!} \leqq \left(\frac{e\xi}{U}\right)^U,$$

$0 < V \leqq \xi$ ならば，

(ii) $$\sum_{0 \leqq d \leqq V} \frac{\xi^d}{d!} \leqq \left(\frac{e\xi}{V}\right)^V.$$

(証明) (i) $0 < \xi \leqq U$ ならば，

$$\sum_{d \geqq U} \frac{\xi^d}{d!} = \sum_{d \geqq U} \frac{U^d}{d!}\left(\frac{\xi}{U}\right)^d \leqq \left(\frac{\xi}{U}\right)^U \sum_{d \geqq U} \frac{U^d}{d!} \leqq \left(\frac{\xi}{U}\right)^U e^U.$$

(ii) $0 < V \leqq \xi$ ならば，

$$\sum_{0 \leqq d \leqq V} \frac{\xi^d}{d!} = \sum_{0 \leqq d \leqq V} \frac{V^d}{d!}\left(\frac{\xi}{V}\right)^d \leqq \left(\frac{\xi}{V}\right)^V \sum_{0 \leqq d \leqq V} \frac{V^d}{d!} \leqq \left(\frac{\xi}{V}\right)^V e^V.$$

以上の準備の下にいよいよ定理A～Cの証明に入る。

§4： 定理 A，B，C の証明．

（定理Aの証明）

$$\alpha = \left\{\frac{1}{2}\left(1+\frac{2}{\pi}\right)\right\}^{\frac{1}{2}}$$ ととると，明かに

(1) $$0 < \alpha < 1 \quad , \quad \frac{\pi}{2}\alpha^2 > 1 \ .$$

となっているから，

(1)′ $$\alpha_1 = \frac{1}{2} \ , \quad \alpha_j = \alpha\left(\frac{\log j}{j}\right)^{\frac{1}{2}} \ , \ (j \geqq 2)$$

とする。 仮定Aが成立していることは明かである。

Lemma 2 において $c = c' = \frac{1}{2}$ の場合であるから，

$$\lambda_n \sim \frac{\pi}{2}\alpha^2 \log n \ .$$

従って，(1)より明かなように，

(2) $$e^{-\lambda_n} \ll n^{-1-\delta} \ ,$$

となる $\delta > 0$ が存在する。

定理Aを，我々は，確率1で

$$\log n \ll r_n(\omega) \ll \log n \ , \quad (n \geqq n_0)$$

となるという形で，即ち， $\lambda'_n \sim \lambda_n \sim \frac{\pi}{2}\alpha^2 \log n$ であるから，

(3) $$\lambda'_n \ll r_n(\omega) \ll \lambda'_n \qquad (n \geqq n_0(\omega))$$

となる形で証明する。

そのために，定理5 を 2度用いる。 即ち，ある正の定数 c', c'' に対して，

(4) $$\sum_{n=1}^{\infty}\mu(\{\omega ; r_n(\omega) > c'\lambda'_n\}) < +\infty ,$$

かつ (5) $$\sum_{n=1}^{\infty}\mu(\{\omega : r_n(\omega) < c''\lambda'_n\}) < +\infty ,$$

であることが証明されれば良い訳である。

所が，Lemma 6 と 8 によって，

$$\mu(\{\omega : r_n(\omega) > c'\lambda'_n\}) \leqslant e^{-\lambda_n}\sum_{d > c'\lambda'_n}\frac{(\lambda'_n)^d}{d!}$$
$$\leqslant e^{-\lambda_n}\left(\frac{e}{c'}\right)^{c'\lambda'_n}$$

が $c' > 1$ ならば成立するから，特に $c' = e$ ととれば，

(2) より (4) が成立することが分る。

次に，再び Lemma 6 と 8 によって，

$$e^{-\lambda_n}\sum_{0 \leqslant d \leqslant c''\lambda'_n}\frac{(\lambda'_n)^d}{d!} \leqslant e^{-\lambda_n}\left(\frac{e}{c''}\right)^{c''\lambda_n}$$

が $0 < c'' < 1$ ならば成立するから，c'' を十分小さくとれば，

$$\left(\frac{e}{c''}\right)^{c''\lambda_n} \leqslant n^{\frac{\delta}{2}}$$

となることが分れば，(2) より (5) が成立する事が示される。

所が，$\lambda'_n \leqslant c^* \log n$ となる正の定数 c^* が存在するから，

$$\left(\frac{e}{c''}\right)^{c''} \leqslant e^{\frac{\frac{\delta}{2}}{c^*}}$$

となる正の定数 $c'' < 1$ が存在することを示せば良い。

これは，
$$\left(\frac{e}{t}\right)^t \to 1 \quad (t \to +0)$$
であることより明かである。 従って(3)が証明された。
以上で我々は，(1)′ のような確率を与えられた殆んどすべての ω （確率空間 $(\Omega, \mathcal{S}, \mu)$ の中で）は定理Aの性質をもっていることが証明できたことになる。

（定理 B の証明）

$\forall \varepsilon > 0$ を与える。 Lemma 2 において
$$\alpha = \frac{1}{2}, \quad c = 1 - \frac{1}{2+\varepsilon}, \quad c' = 0$$
とおけば，仮定Aが成立し，確率 1 で
$$a_j \sim c^* j^{2+\varepsilon}$$
が成立している。 そして

(6) $$\lambda_n' \sim \lambda_n \sim c^{**} n^{-\frac{\varepsilon}{2+\varepsilon}} .$$

そこで，もしある数 K に対して

(7) $$\sum_{n=1}^{\infty} \mu(\{\omega : r_n(\omega) \geqq K\}) < +\infty$$

となるならば， $\lambda_n \to 0$ ，$\lambda_n' \to 0$ であるから，
Lemma 6 によって，

(8) $$e^{-\lambda_n} \sum_{d \geqq K} \frac{(\lambda_n')^d}{d!} \ll e^{-\lambda_n}\left(\frac{e\lambda_n'}{K}\right)^K \ll (\lambda_n')^K$$

が十分大きい n に対して成り立つ。
従って，

$$K\frac{\varepsilon}{2+\varepsilon} > 1$$

即ち　　$$K > 1 + \frac{2}{\varepsilon}$$

ととれば，(6)(8) より明かに (7) が成立することが訳る。

よって，確率 1 で，

$$r_n(\omega) < 2\left(1+\frac{1}{\varepsilon}\right), \quad (n \geqq n_1(\varepsilon,\omega))$$

となる。 これは定理 B の主張を含んでいること明かである。

（定理 C の証明）

$$\alpha_j = \begin{cases} \frac{1}{2} & \cdots\cdots\cdots \quad 1 \leqq j < j_0 \\ \alpha \frac{\log j}{j} & \cdots\cdots\cdots \quad j \geqq j_0 \end{cases}$$

とする。 ここに， α は後に定める正の定数であって，$j_0 = j_0(\alpha)$ は， $j_0 \geqq 3$ であって，$0 < \alpha_j < 1$ $(j \geqq 1)$ となるようにとるものとする。

このとき明かに仮定 A が成立し，Lemma 3 より

(9) $$S_n^*(\omega) \sim \sum_{j=1}^{n} \alpha_j \sim \frac{\alpha}{2}(\log n)^2 .$$

そこで，いま $n \in \mathcal{N}$ を

$$n = p + b \qquad (p \in \mathfrak{P},\ b \in \omega)$$

と表わす表わし方の個数を $R_n(\omega)$ とすると，明かに

$$R_n(\omega) = \sum_{p<n} \rho_{n-p}(\omega) .$$

そして，

$$\Lambda_n = M\{R_n(\omega)\} = \sum_{p<n} \alpha_{n-p}\ .$$

Lemma 4，6 において $d=0$ とすると，

$$\mu(\{\omega : R_n(\omega)=0\}) = \prod_{p<n} (1-\alpha_{n-p})\ .$$

$$(5) \quad \therefore \mu(\{\omega : R_n(\omega)=0\}) \leqq e^{-\Lambda_n}\ .$$

そこで，もし

$$(6) \qquad \sum_{n=1}^{\infty} \mu(\{\omega : R_n(\omega)=0\}) < +\infty$$

ならば，定理5 によって，確率 1 で

$$R_n(\omega) > 0 \qquad (n \geqq n_0)$$

となり，(4) が保証される。

(6) の成立には，(5) より，

$$e^{-\Lambda_n} \ll n^{-1-\delta}$$

なる正数 δ が存在することを示せば十分である。

次に我々は，α を選ぶ事によって，

$$\Lambda_n > 2\log n\ , \qquad (n \geqq n_0)$$

となること，従って $\delta = 1$ ととれることを示す。

そのために，次の Hoheisel の定理を用いる。

［定理］（Hoheisel：Sitzungsber. Berlin (1930) 580～88）

$$\sum_{\substack{m<p\leqq m+m^c \\ p\in\mathfrak{P}}} 1 \sim \frac{m^c}{\log m} \qquad (m\to\infty)$$

となるような絶対定数 c $(0<c<1)$ が

存在する。

従って，特に，

$$\sum_{m<p\leqq m+m^c} 1 > \frac{2}{3}\cdot\frac{m^c}{\log m}, \quad (m \geqq m_0).$$

いま， $m<p\leqq m+m^c \quad (0<c<1)$ を満足する

自然数 m の個数 M を考えると，

$$p-p^c<p-m^c\leqq m\leqq p-1,$$

であるから，Mは

$$p-p^c\leqq m\leqq p-1$$

を満足する m の個数を越えない。

よって， $$\sum_{\substack{m \\ m<p\leqq m+m^c}} 1 \leqq p^c$$

$$\therefore\ p^{-c}\sum_{\substack{m \\ m<p\leqq m+m^c}} 1 < 1.$$

これより，

$$\Lambda_n=\sum_{p<n}\alpha_{n-p} \geqq \sum_{p<n}\alpha_{n-p}\,p^{-c}\sum_{\substack{m \\ m<p\leqq m+m^c}} 1.$$

$l=l(n)=[n^c]$ とすると，

$$\Lambda_n \geqq \sum_{m=m_0}^{n-2l}\ \sum_{\substack{p \\ m<p\leqq m+m^c}} \alpha_{n-p}\,p^{-c}.$$

そして，nは十分大で $n-p \geqq j_0$ となるから，α_j の単調減少性と Hoheisel の定理とによって，

$$\Lambda_n \geqq \sum_{m=m_0}^{n-2l} \alpha_{n-m} (2m)^{-c} \sum_{\substack{p \\ m<p\leqq m+m^c}} 1 .$$

$$\geqq \sum_{m=m_0}^{n-2l} \alpha_{n-m} (2m)^{-c} \left(\frac{2}{3} \cdot \frac{m^c}{\log m}\right)$$

$$> \frac{1}{3\log m} \sum_{m=m_0}^{n-2l} \alpha_{n-m} = \frac{1}{3\log m} \sum_{j=2l}^{n-m_0} \alpha_j .$$

一方，$l = [n^c] \sim n^c \quad (n \to \infty)$ であるから，

$$\sum_{j=2l}^{n-m_0} \alpha_j \sim \frac{\alpha}{2}(1-c^2)\cdot(\log n)^2$$

であり，また $1-c^2 > 1-c$ であるから，結局

$$\Lambda_n > \frac{\alpha}{6}(1-c)\log n \quad , \quad (n \geqq n_0)$$

となる。 そこで $\alpha = \dfrac{12}{1-c}$ ととれば

$$\Lambda_n > 2\log n \qquad (n \geqq n_0)$$

となって，我々の証明すべき結果が得られた。

q. e. d.