4.3.2021

Chapter II

"Classical" probabilistic number theory

1. Distribution of additive functions

Euler function : "multiplicative"

Def. (1) $f : \{1, 2, \dots\} \longrightarrow \mathbb{C}$ is **multiplicative** if

$$f(mn) = f(m) f(n), \quad \text{if } m \text{ and } n \text{ are coprime}$$

[**Ex:** $\varphi(n)$; $\varphi(mn) = \varphi(m)\varphi(n)$, if $(m,n) = 1$ ($\gcd = 1$)

but not for all m, n:

$$\varphi(p^2) = p^2 - p \neq (p-1)^2$$

(2) f is called **additive** if

$$f(mn) = f(m) + f(n), \quad \text{if } (m,n) = 1$$

Examples:

(1) $f(n) = \log\left(\frac{\varphi(n)}{n}\right)$ is additive

(2) $f(n) = \log(n)$ " "

(3) $f(n) = \omega(n) =$ nb. of primes $p \mid n$, without multiplicity

is additive

(4) Most generally: f additive

$$f(n) = \sum_{p^\nu \| n} f(p^\nu)$$

"exact division", $p^\nu \mid n$, $p^{\nu+1} \nmid n$

Conversely: for arbitrarily chosen $a_{p^\nu} \in \mathbb{C}$ for every prime p and $\nu \geq 1$, defining

$$f(n) = \sum_{p^\nu \| n} a_{p^\nu}$$

gives an additive function.

Theorem (Erdős – Wintner; ~1939)

$\Omega_N = \{1, \dots, N\}$

$\mathbb{P}_N(x) = \frac{1}{N}$, $x \in \Omega_N$

f additive function

The r.v. $\left(\underline{F}_N : n \longmapsto f(n) \right)$ on Ω_N

converge in law $\Leftrightarrow$ the three series

$$\sum_{|f(p)| \leq 1} \frac{f(p)}{p} \quad ; \quad \sum \frac{|f(p)|^2}{p} \quad ; \quad \sum_{|f(p)| > 1} \frac{1}{p}$$

$|f(p)| \leq 1$ $\qquad$ $|f(p)| \leq 1$ $\qquad$ $|f(p)| > 1$

converge.

1 can be replaced by any fixed $c > 0$

When this is the case, the limit is

$$F = \sum_p f(p^{V_p})$$

where $(V_p)_p$ is a sequence of independent geometric r.v. with parameter $1 - \frac{1}{p}$, i.e.

$(k \geq 0)$ $\quad \mathbb{P}(V_p = k) = \left(1 - \frac{1}{p}\right) p^{-k}$.

Ex. (1) $f(n) = \log\left(\frac{\varphi(n)}{n}\right)$

$$f(p) = \log\left(1 - \frac{1}{p}\right) \sim -\frac{1}{p}$$

$\Rightarrow$ The three series converge

(2) $f(n) = \omega(n)$: $f(p) = 1$, and

the first two series do not converge

because of

Th. (Euler) $\sum_{\substack{p \\ \text{prime}}} \frac{1}{p} = +\infty$.

In fact:

Th. (Mertens; Chebychev)

$$\sum_{p \le x} \frac{1}{p} = \log\log(x) + O(1)$$

$f \ll g$, $f = O(g)$ $\Leftrightarrow$ $|f(x)| \le C g(x)$ for some $C > 0$

[Digression: proof of Euler's Th.

Consider: $\prod_{p \le x} \frac{1}{1 - \frac{1}{p}}$ for $x \geq 2$

$$= \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^h} + \cdots \right)$$

$$= \sum_{d \geq 1}{}' \frac{1}{d} \geq \sum_{d \le x} \frac{1}{d}$$

$(p \mid d \Rightarrow p \le x)$ $\quad = \log(x) + O(1)$

$$\Rightarrow \quad - \sum_{p \le x} \log\left(1 - \frac{1}{p}\right) \geq \log\log(x) + O(1)$$

$$\left[\sum_{p \le x} \frac{1}{p} + \underbrace{O\left(\sum_{p \le x} \frac{1}{p^2} \right)}_{= O(1)} \right]$$

(3) If $|f(p)| \le \frac{1}{p^\alpha}$ for some $\alpha > 0$,
then the three series converge;

since $\sum \frac{1}{n^{1+\alpha}}$, $\sum \frac{1}{n^{1+2\alpha}}$ are.

Motivation for the limit

$$f(n) = \sum_{p^\nu \| n} f(p^\nu)$$

$$= \sum_p f\left(p^{\nu_p(n)}\right)$$

where $\nu_p(n)$ = p-adic valuation
= exponent of p in the factor. of n

(note $f(1) = 0$)

Now note :

Lemma - $(\nu_p)_p$ on Ω_N converges in law to $(\nu_p)_p$, ind. geometric r.v, as in the statement.

[meaning $(\nu_p)_{p \le M} \downarrow$ law $(\nu_p)_{p \le M}$]

Proof - Direct application of Th. 1.3.1 + Cor. : for instance

$$\{ v_p = k, \quad v_q = \ell \}_{\Omega_N} \qquad [p \neq q]$$

$$\| $$

$$\{ n \bmod p^{k+1} \in \{ x \bmod p^{k+1} \mid x \neq 0, \; x = 0 \bmod p^k \}$$

and

$$\{ n \bmod q^{\ell+1} \in \dots \}_{\Omega_N}$$

which has probability tending to

$$\left(\frac{1}{p^{k+1}} (p-1) \right) \times \left(\frac{1}{q^{\ell+1}} (q-1) \right)$$

$$\|$$

$$\frac{1}{p^k}\left(1 - \frac{1}{p}\right) \times \frac{1}{q^\ell}\left(1 - \frac{1}{q}\right)$$

$$\|$$

$$P(v_p = k \text{ and } v_q = \ell)$$

□

One can expect that if there is convergence, the limit must be

$$F = \sum_p f(p^{v_p}).$$

One can determine when the series exist by using Kolmogorov's Th. of F. Assume $|f| \leq 1$, Then the conv. in law is equivalent to convergence of

$$\sum_p \mathbb{E}\left(f(p^{V_p})\right)$$

and $$\sum_p \mathbb{V}\left(f(p^{V_p})\right).$$

Note that

$$\mathbb{E}\left(f(p^{V_p})\right) = \sum_{k \geq 0} f(p^k)\,\frac{1}{p^k}\left(1 - \frac{1}{p}\right)$$

$$= \sum_{k \geq 1} \frac{f(p^k)}{p^k} - \sum_{k \geq 1} \frac{f(p^k)}{p^{k+1}}$$

so

$$\sum_p \mathbb{E}\left(f(p^{V_p})\right) = \sum_p \frac{f(p)}{p} - \sum_{k \geq 2} \frac{f(p^k)}{p^k}$$

$$= \sum_p \frac{f(p)}{p} \quad \text{(1st series in E-W theorem)} + (\ldots) + O\left(\sum_{n \geq 1} \frac{1}{n^2}\right) + (\ldots)$$

Similar for the $\sum V(\_)$ and the second E-W series.

Proof of convergence in Erdős-Wintner

Assume that $|f| \le C$ for some C

and $f(p^k) = 0$ if $k \ge 2$.

Idea: again use Th. B.4.4 as in Schoenberg's Th:

$$\underline{F}_N(n) = f(n) = \sum_p f\left(p^{\underline{V}_p(n)}\right)$$

so we approximate $\underline{F}_N$ by

$$\underline{F}_{N,M} = \sum_{p \le M}{}' f\left(p^{\underline{V}_p}\right)$$

Step 1.

Fix M. By the lemma above, [and the composition principle] we get

$$\underline{F}_{N,M} \xrightarrow[N\to\infty]{\text{law}} \sum_{p \le M} f\left(p^{V_p}\right) \overset{!!}{:=} G_M$$

[So if the series $\overset{F}{\checkmark}$ converges, it is the limit of G_M]

This gives the 1st assumption in B.9.4

Step 2. Goal:

$$\lim_{M\to\infty} \overline{\lim_{N\to\infty}} \mathbb{E}_N\left(|\underline{E}_{N,M}|\right)$$

where $$\underline{F}_N = \underline{F}_{N,M} + \underline{E}_{N,M}$$

We have

$$\underline{E}_{N,M} = \sum_{p>M} f\left(p^{\underline{v}_p}\right)$$

Triangle inequality does not work here.

Next idea: use Cauchy-Schwarz inequality

$$\mathbb{E}_N\left(|\underline{E}_{N,M}|\right)^2 \le \mathbb{E}_N\left(|\underline{E}_{N,M}|^2\right)$$

Further:

$$\mathbb{E}_N\left(\left|\sum_{p>M} f\left(p^{\underline{v}_p}\right)\right|^2\right)$$

$$= \sum_{p_1, p_2 > M} \mathbb{E}_N \left(f(p_1^{\nu_{p_1}}) \overline{f(p_2^{\nu_{p_2}})} \right)$$

$$= \sum_{p_1, p_2 > M} f(p_1) \overline{f(p_2)} \, \mathbb{P}_N \left(\nu_{p_1} = \nu_{p_2} = 1 \right)$$

(because $f(p^\nu) = 0$ unless $\nu = 1$)

Two cases:

$p_1 = p_2$: then we get

$$\sum_{p > M} |f(p)|^2 \underbrace{\mathbb{P}_N \left(\nu_p = 1 \right)}_{= \frac{1}{N} \left| \left\{ n \le N \,/\, p \mid n \text{ and } p^2 \nmid n \right\} \right|}$$

$$\le \frac{1}{N} \frac{N}{p}$$

$$= \sum_{p > M} \frac{|f(p)|^2}{p} \left(\xrightarrow[M \to \infty]{} 0 \text{ by the convergence } \sum_p \frac{|f(p)|^2}{p} \right)$$

OK

$p_1 \neq p_2$:

neglect

$$\sum_{\substack{p_1, p_2 > M \\ p_1 \neq p_2}} f(p_1)\overline{f(p_2)} \; \Pi_N\big(p_1 p_2 \mid n \; [\text{but } p_1^2 \nmid n,\ p_2^2 \nmid n]\big)$$

$$= \frac{1}{p_1 p_2} + O\left(\frac{1}{N}\right)$$

by Th. 1.3.1

and $= 0$ if $p_1 p_2 > N$

Therefore the contribution of $p_1 \neq p_2$ is:

$$\sum_{\substack{p_1, p_2 > M \\ p_1 p_2 \leq N \\ p_1 \neq p_2}} \frac{f(p_1)\overline{f(p_2)}}{p_1 p_2} + O\left(\frac{1}{N} \sum_{\substack{p_1, p_2 > M \\ p_1 p_2 \leq N}} |f(p_1) f(p_2)|\right)$$

$$= \left| \sum_{p > M} \frac{f(p)}{p} \right|^2 - \sum_{p > M} \frac{|f(p)|^2}{p^2} + O\left(\frac{\quad}{\quad}\right)$$

$$\leq \left| \underbrace{\sum_{p>M} \frac{f(p)}{p}} \right|^2$$

$\longrightarrow 0$ by convergence of the 1st series

$$+ \quad O$$

$$+ \quad O\left(\underbrace{\frac{1}{N} \left| \{ p_1 p_2 \leq N \} \right|}_{\text{forgot that } p_i > M} \right)$$

Lemma- For $N \geq 1$,

$$\frac{1}{N} \left| \{ n \leq N \mid \underbrace{n = p_1 p_2}_{n = p} \} \right| = O\left(\frac{\log \log N}{\log N} \right)$$

$$= O\left(\frac{1}{\log N} \right)$$

[This is at the level of Mertens - Chebychev - type bounds]

Conclusion:

$$\mathbb{E}_N\left(|E_{N,M}|^2\right) \leq \sum_{p>M} \frac{|f(p)|^2}{p} + \left|\sum_{p>M} \frac{f(p)}{p}\right|^2 + O\left(\frac{\log\log N}{\log N}\right)$$

so $\overline{\lim_{N\to\infty}} \ldots \leq$ // + //

$$\Rightarrow \lim_{M\to\infty} \overline{\lim_{N\to\infty}} (\ldots) = 0$$

by convergence of the 1st two series in $E-W$.

Hence (B.4.4) we get

$$F_N \xrightarrow{\text{law}} \lim_{M\to\infty} C_M = \sum_p f(p^{\nu_p})$$

□