22.2.2021

Probabilistic Number Theory

Outline:

1. Introduction
2. Erdős - Kac Theorem
3. Chebychev Bias
4. Riemann zeta function
5. Exponential sums
6. Chinese Remainder Theorem

Chapter I

Introduction

1. Why does probabilistic nb. theory even exist?

Number Theory : properties of

integers
prime numbers
solutions of equations, for instance n^2+m^2
:

which are deterministic.

But for instance knowing the number of primes p dividing

$$N = 123456789101112\ldots25$$

of $N+1$? $N+2$?

This is difficult to predict.

Q. What happens on average?

One sees regularity appearing.

Focus:

The asymptotic behavior of sequences of arithmetically-defined random variables

Exemple. (Erdős-Kac, 1939)

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

$\mathbb{P}_N$ = uniform prob., $\mathbb{P}_N(a) = \frac{1}{N}$

$\omega_N : n \longmapsto$ nb. of $p \mid n$ (w.o. multiplicity)

Then

$$\frac{\omega_N - \log\log N}{\sqrt{\log\log N}} \xrightarrow[N\to\infty]{\text{law}} \mathcal{N}(0,1)$$

i.e.

$$\lim_{N\to\infty} \frac{1}{N} \left| \left\{ n \leq N \;/\; a < \frac{\omega_N(n) - \log\log N}{\sqrt{\log\log N}} < b \right\} \right|$$

Set: X

$|X|$ = nb. of elements

$$= \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2}\, dt$$

for all $a < b$.

(In particular: a "typical" integer has many prime factors)

Application: "multiplication table problem" (Erdős)

Write

	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

N^2 numbers

ab

with $1 \leq a, b \leq N$

How many distinct numbers arise?

(say $m(N)$)

$$\lim_{N \to \infty} \frac{m(N)}{N^2} = 0.$$

Why ? a typical integer

$$1 \leq a \leq N$$

has $\approx$ loglog N prime factors

and the same for $1 \leq b \leq N$

$\Rightarrow$ ab has about

$$2 \log\log N$$

prime divisors

But $\log\log N^2 \simeq \log\log N$

so the ab are very "atypical"

$\Rightarrow$ negligible proportion.

2 - Convergence in law

Def. $(\Omega_n, \Sigma_n, \mathbb{P}_n)$ proba. spaces

(M, d) metric space

[ex. $\mathbb{R}$, $\mathbb{R}^d$]

$X_n : \Omega_n \longrightarrow M$

random variables

X r.v. with values in M

or

μ prob measure on M

Then $X_n \xrightarrow{\text{law}} X$

$[\ X_n \xrightarrow{\text{law}} \mu\ ]$

$\Leftrightarrow \forall\ f : M \longrightarrow \mathbb{C}$ continuous and bounded

we have

$$\mathbb{E}_n(f(X_n)) \xrightarrow[n \to +\infty]{} \mathbb{E}(f(X))$$

$$\left[\text{or} \quad \int_M f(x)\, d\mu(x)\right]$$

Corollary ("mapping principle")

If $X_n \xrightarrow{\text{law}} X$, X M-valued

and $\varphi : M \longrightarrow \mathbb{C}$ continuous

[N metric]

then $\varphi(X_n) \xrightarrow{\text{law}} \varphi(X)$

3_ Integers in arithmetic progressions

Th. [1.3.1]

$N \geq 1$, Ω_N, $\mathbb{P}_N$ as above

$q \geq 1$, $\pi_q : \mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ projection

$X_N(n) = \pi_q(n)$, $\underbrace{\mathbb{Z}/q\mathbb{Z}}_{\text{discrete}}$ - valued

Then

$$X_N \xrightarrow{\text{law}} \mu_q = \text{uniform prob. on } \mathbb{Z}/q\mathbb{Z}$$

More precisely for

$$f : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{C}$$

we have

$$\left| \mathbb{E}_N(f(X_N)) - \frac{1}{q}\sum_x f(x) \right| \leq \frac{2}{N} \|f\|_1$$

where

$$\|f\|_1 = \sum |f(x)|$$

Proof :

$$\mathbb{E}_N(f(X_N)) = \frac{1}{N} \sum_{n \le N} f(n \bmod q)$$

$$= \sum_{0 \le x \le q-1} f(x) \; \frac{1}{N} \sum_{\substack{n \le N \\ n \equiv x \bmod q}} 1$$

$$n = x + mq,$$

$$\frac{1-x}{q} \le m \le \frac{N-x}{q}$$

$$= \sum_{0 \le x \le q-1} f(x) \cdot \frac{1}{N} \cdot \left(\frac{N}{q} + (\le 1) \right)$$

$$= \frac{1}{q} \sum_{x} f(x) + \left(\text{at most } \frac{2}{N} \sum |f(x)| \right)$$

□

[1.3.7]

Corollary - Let

$$q_1, \dots, q_r \geq 1$$

pairwise coprime. Then

$$(n \in \Omega_N) \longmapsto (n \bmod q_1, \dots, n \bmod q_r)$$

$$\uparrow$$

$$\prod_i \mathbb{Z}/q_i\mathbb{Z}$$

converge in law to

$$(X_1, \dots, X_r)$$

where X_i is uniform mod q_i

and $(X_1, \dots, X_r)$ are independent.

Proof - Chinese Remainder Th:

$$\mathbb{Z}/q_1 \cdots q_r\mathbb{Z} \xrightarrow{\sim} \prod_i \mathbb{Z}/q_i\mathbb{Z}$$

$$n \longmapsto (n \bmod q_1, \dots, n \bmod q_r)$$

and $\mu_{q_1 \cdots q_r} \longleftrightarrow \underbrace{\bigotimes_i \mu_{q_i}}_{\text{law of } (X_1, \ldots, X_r)}$

The so-called random vectors above correspond to $n \longmapsto n \bmod q_1 \cdots q_r$ and so $\xrightarrow{\text{law}} \mu_{q_1 \cdots q_r}$ by 1.3.1.

□

4. Schoenberg's theorem

Def ["Euler function"] $\varphi(n) = \left| \left(\mathbb{Z}/n\mathbb{Z} \right)^{\times} \right|$ (units)

$= \left| \{ 1 \le a \le n \mid a \text{ coprime to } n \} \right|$

Formula: $\varphi(n) = n \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p} \right)$

Ex. $\varphi(p) = p - 1$

$n \geq 1$, $\varphi(p^n) = p^n - p^{n-1}$

$= p^n \left(1 - \frac{1}{p}\right)$

[1.4.1]

Th. (Schoenberg, 1928)

Ω_N, $\mathbb{P}_N$

$F_N(n) = \frac{\varphi(n)}{n}$, $0 \leq F_N \leq 1$

$F_N \xrightarrow{\text{law}} F$

where

$$F = \prod_{p \text{ — primes}} \left(1 - \frac{B_p}{p}\right)$$

where

$(B_p)_p$ are independent Bernoulli with

$\mathbb{P}(B_p = 1) = \frac{1}{p}$.

The product converges a.s. (almost surely)