DIRICHLET’S THEOREM ON ARITHMETIC PROGRESSION

SIYUN KIM

TABLE OF CONTENTS

GENERATING FUNCTION

- Motivation
- Definition
- Examples
- Dirichlet series

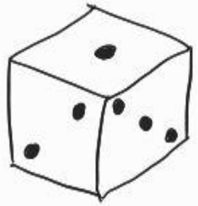
For a given sequence $\{a_n\}_{n\in\mathbb{N}}$,

A generating function of the sequence $\{a_n\}_{n\in\mathbb{N}}$ is

$$\sum_{n=0}^{\infty} a_n f_n(x)$$

In general, $f_n(x) = x^n$.

For example,

 $\times 2 \longmapsto (z + z^2 + z^3 + z^4 + z^5 + z^6)^2 = \sum_{n=2}^{12} a_n z^n$

Lagrange's four-square theorem:

$n = a^2 + b^2 + c^2 + d^2$

$\longmapsto (1 + z + z^{2^2} + z^{3^2} + \cdots)^4 = \sum_{n=0}^{\infty} a_n z^n$ s.t. $a_n \neq 0 \ \forall n$

For example,

Fibonacci sequence

$$F_{n+2} = F_{n+1} + F_n,\ F_0 = 0,\ F_1 = 1 \longmapsto F(x) := \sum_{n=0}^{\infty} F_n \frac{x^n}{n!} \quad \text{s.t.} \quad F''(x) = F'(x) + F(x),\ F(0) = 0,\ F'(0) = 1.$$

Prime number sequence

$$(2, 3, 5, 7, \cdots) \longmapsto \ ?$$

CONSTRUCTION OF GENERATING FUNCTION 1: PRIME NUMBERS

- Unique factorization theorem
- Euler's product formula
- Riemann zeta function
- Corollary : there are infinitely many prime numbers

Idea 1: Unique Factorization Theorem

$$n = \prod_{i=1}^{m} p_i^{r_i}$$

Euler's product:

Let $f_n(z) = e^{-z \cdot \log n}$. Then, $\sum_{n=1}^{\infty} f_n(z) = \prod_{p} \left(1 - e^{-z \cdot \log p}\right)^{-1}$!

Idea II: Uniform convergence and Logarithm

$\sum_{n=1}^{\infty} f_n(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$ converges uniformly on $z>1$. Define a function $\zeta(z)$ on $z>1$ by

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \quad (z>1)$$

Since $\zeta(z)>0$ on $z>1$,

$$\log \zeta(z) = \sum_{p} \left(1-e^{-z\log p}\right)^{-1}, \quad \therefore \log \zeta(z) = \sum_{p} \sum_{m=1}^{\infty} \frac{1}{m} \left[e^{-z\log p}\right]^{m}$$

Hence

$$\log \zeta(z) = \sum_{p^m} \frac{1}{m} e^{-z \cdot \log p^m} = \sum_{p} \frac{1}{p^z} + \sum_{p^m,\, m \geq 2} \frac{1}{m \cdot p^{mz}}$$

We conclude that

$$\lim_{z \to 1+} \sum_{p} \frac{1}{p^z} = \infty$$

ARITHMETIC PROGRESSION

- Motivation
- Definition
- What is the condition of arithmetic progression to have many prime numbers?
- Dirichlet's theorem on arithmetic progression

Is there any "pattern" of prime numbers?

Explicit formula of $n \mapsto p_n$

What about converse? $p_n \mapsto n$ (Distribution)

Reducing the size of $\mathbb{N}$: Arithmetic progression $\{a + (n-1)q\}_{n \in \mathbb{N}}$ (a, q)

CONSTRUCTION OF GENERATING FUNCTION 11: PRIME NUMBERS IN ARITHMETIC PROGRESSION 1: PRIME MODULOUS

- Analogous on Riemann zeta function
- Multiplicative arithmetic function
- 1 on the desired prime numbers and 0 for the others
- Motivation for character

$$\sum_{n=1}^{\infty} f(n) \cdot e^{-z \cdot \log n} = \prod_{p} \left(1 - f(p) e^{-z \cdot \log p}\right)^{-1} \quad \left(f(p^m) = [f(p)]^m \right)$$

$$\downarrow$$

$$\sum_{f} \sum_{p} \sum_{m=1}^{\infty} \frac{1}{m} f(p^m) e^{-z \cdot \log p^m} = \sum_{p^m;\ p^m \equiv a \pmod{q}} \frac{1}{m} e^{-z \cdot \log p^m} \quad \left(\text{How to construct } f\,?\right)$$

$$f_k(n) = \begin{cases} \chi_k^{\nu(n)} & (n, q) = 1 \\ 0 & (n, q) > 1 \end{cases}$$, where χ_k's are characters of $\mathbb{Z}_q^\times$. That is, $\chi_k = \chi(k) = e^{\frac{2\pi i}{q-1}(k-1)}$

$$\rightarrow \frac{1}{q-1} \sum_{k=1}^{q-1} \sum_{p} \sum_{m=1}^{\infty} \frac{1}{m} f_k(p^m) e^{-z \cdot \log p^m} = \sum_{p^m,\, p^m \equiv a \pmod{q}} \frac{1}{m} e^{-z \cdot \log p^m}$$

$$L_k(z) = \sum_{n=1}^{\infty} f_k(n) e^{-z \cdot \log n} \quad (z > 1,\ k = 1, 2, \cdots, q-1)$$

Note that $L_1(z) = (1 - e^{-z \log q}) \zeta(z)$ (principal character)

Proof of boundedness of characters other than principal characters:

$$\frac{1}{q-1}\sum_{k=1}^{q-1} \mathrm{Log}\, L_k(z) = \sum_{p} \frac{1}{p^z} + O(1) \geq 0$$

$$\prod_{k=1}^{q-1} L_k(z) \geq 1 \quad \text{for } z>1 \quad \text{and} \quad L_1(z) < \frac{z}{z-1}\left(1-e^{-z\log q}\right)$$

By Dirichlet's test for convergence,

$$L_k(z) \text{ convergence uniformly on } z > 0 \text{ for } k \neq 1$$

If $L_k(1) = 0$ for $k > 1$, then $L_{q+1-k}(1) = 0$. So $\lim\limits_{z \to 1} \prod\limits_{k=}^{q-1} L_k(z) = 0 \geq 1$: $\lightning$

For the case $k = \frac{q+1}{2}$,

$$L_k(1) = \sum_{n=1}^{\infty} \left(\frac{n}{q}\right) e^{-z \cdot \log n}.$$ How to deal with $\left(\frac{n}{q}\right)$?

PRIMITIVE ROOT, INDEX, AND CHARACTER

- Review: primitive root, index
- Definition of character on residue classes of prime modulous
- Definition of Dirichlet character and Dirichlet L-series
- Dirichlet L-function and desired equality
- Proof of divergence at s=1

LEGENDRE SYMBOL AND GAUSSIAN SUMMATION

- For the case w=-1
- Case 1: q=1 (mod 4)
- Case 11: q=3 (mod 4)

Gaussian sum.

$$G(n) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e^{\frac{2\pi m i}{q} \cdot n}$$

Since $[G(1)]^2 = \begin{cases} q & q \equiv 1 \pmod 4 \\ -q & q \equiv 3 \pmod 4 \end{cases}$

$$L_1(z) = \begin{cases} -\frac{\pi}{\sqrt{q}} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \log\left(2\sin\frac{m\pi}{q}\right) & q \equiv 1 \pmod 4 \text{ : } \underline{\text{Cyclotomy}} \\ -\frac{\pi}{q\sqrt{q}} \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) m & q \equiv 3 \pmod 4 \text{ : Odd} \end{cases}$$

Hence $$\frac{\prod_N \sin\left(\frac{N}{q}\pi\right)}{\prod_R \sin\left(\frac{R}{q}\pi\right)} \doteq \frac{\prod_N \left(1-\zeta^N\right)}{\prod_R \left(1-\zeta^R\right)} = \frac{Y(1)-\sqrt{q}\cdot Z(1)}{Y(1)+\sqrt{q}\cdot Z(1)} \neq 0 \quad (\because Z(1)\neq 0)$$

$\blacksquare$

CONSTRUCTION OF GENERATING FUNCTION II: PRIME NUMBERS IN ARITHMETIC PROGRESSION II: COMPOSITE MODULUS

- Analogous on prime modulus
- Definition of character and existence of primitive roots
- Induce desired inequality by properties of Dirichlet characters

Generalization of q (may not be a prime):

$$q = 2^r p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

$$\chi_k^{L(n)} \longrightarrow \chi(n\,;2^r)\,\chi(n\,;p_1^{r_1})\,\chi(n\,;p_2^{r_2})\cdots\chi(n\,;p_m^{r_m})$$

$$f_k(n) \longrightarrow f_\chi(n) = \begin{cases} \overline{\chi(a)}\,\chi(n) & (n,q)=1 \\ 0 & (\text{otherwise}) \end{cases}$$

$$L_K(z) \to L(z,\chi) = \sum_{n=1}^{\infty} \chi(n) e^{-z \cdot \log n}$$

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \operatorname{Log} L(z,\chi) = \sum_{\substack{p \\ p \equiv a \pmod q}} \frac{1}{p} + O(1)$$

The corresponding remaining to do is

$$\underline{L(1,\chi)} \neq 0 \quad \text{for } \chi \neq \chi_0$$

Proof of boundedness of characters other than principal characters:

For the case of complex characters, using conjugation,

$$\prod_{\chi} |L(z, \chi)| \geq 1 \quad \text{for} \quad z > 1$$

Proof of boundedness of characters other than principal characters:

For the case of complex characters, using conjugation,

$$\prod_{\chi} |L(z,\chi)| \geq 1 \quad \text{for} \quad z > 1$$

What about real characters?

$$\text{W.T.S } L(1,\chi) \neq 0$$

What about real characters? W.T.S $L(1,\chi) \neq 0$

$$\zeta(z) = \sum_{n=1}^{\infty} e^{-z \cdot \log n} \fallingdotseq \frac{z}{z-1} - z\,G(z) \quad \left(G(z) : \text{convergent on } \operatorname{Re} z > 0 \right)$$

ANALYTIC CONTINUATION AND PROOF OF DIVERGENCE

- Extending to complex variables : zeros and singularities
- Cauchy integral formula and induced contradiction

So

$$\mathcal{L}(z,\chi_0) = \frac{\phi(q)}{q}\zeta(z)$$

Analogously, $\chi \neq \chi_0$,

$$\mathcal{L}(z,\chi) = \sum_{n=1}^{\infty} S(n)\left[n^{-z} - (n+1)^{-z}\right] \quad \text{where } S(x) = \sum_{n \leq x} \chi(n)$$

$$= z \cdot \int_1^{\infty} S(x)\, x^{-(z+1)}\, dx \quad \left(S(x) \text{ is bounded since } \sum_n \chi(n) = 0 \right)$$

Suppose that $L(1,\chi)=0$ for real $\chi \neq \chi_0$. Then?

$$\psi(z) := \frac{L(z,\chi)\,L(z,\chi_0)}{L(2z,\chi_0)} \longrightarrow 0 \text{ as } z \longrightarrow \tfrac{1}{2}+ \quad \left(\operatorname{Re} z > \tfrac{1}{2}\right)$$

$$\psi(z) = \prod_{\chi(p)=-1} \frac{\left(1+e^{-z\cdot\log p}\right)^{-1}\left(1-e^{-z\cdot\log p}\right)^{-1}}{\left(1-e^{-2z\cdot\log p}\right)^{-1}} \prod_{\chi(p)=1} \frac{\left(1-e^{-z\cdot\log p}\right)^{-2}}{\left(1-e^{-2z\cdot\log p}\right)^{-1}}$$

$$\prod_{\chi(p)=1}\left(1+2e^{-z\cdot\log p}+2e^{-z\cdot\log p^2}+\cdots\right) = \sum_{n=1}^{\infty} a_n \cdot e^{-z\cdot\log n}$$

with $a_n \geq 0$ and $a_1 = 1$ for $\mathrm{Re}\, z > 1$

$$\therefore \ \psi(z) = \sum_{m=0}^{\infty} \frac{\psi^{(m)}(2)}{m!} (z-2)^{m} \quad \text{on } |z-2| < \frac{3}{2}$$

$$\psi^{(m)}(2) = \sum_{n=1}^{\infty} a_n \cdot (-\log n)^{m} \cdot n^{-2} = (-1)^{m} \cdot b_m \quad \text{with } b_m \geq 0$$

Hence

$$\psi(z) = \sum_{m=0}^{\infty} \frac{(-1)^m b_m}{m!}(z-2)^m = \sum_{m=0}^{\infty} \frac{b_m}{m!}(2-z)^m \quad \text{for } \tfrac{1}{2} < z < 2$$

$$\psi(s) \geq \psi(2) = b_0 = \sum_{n=1}^{\infty} \frac{a_n}{n^2} \geq 1 \quad (\because a_1 = 1) \quad \therefore \lightning$$

Finally,

$$L(1,\chi) \neq 0 \text{ for all } \chi$$

We have completed the proof of Dirichlet's theorem on arithmetic progression!

In the view of distribution, prime numbers are evenly distributed in any arithmetic progression where $(a, q) = 1$.

DISTRIBUTION OF PRIME NUMBERS

- Prime number theory
- Waring's problem
- Riemann hypothesis
- Twin prime conjecture
- James Maynard's accomplishment