数物系サーバー　新歓イベント 2022

解析的整数論入門
リーマン·ゼータ関数 $\zeta(s)$ と愉快な仲間たち

ぱい

Twitter: @END_OF_PAIOTU

2022 年 4 月 17 日　20:00〜21:30

解析的整数論入門

ぱい

自己紹介

- 名前:
  ぱい
- 経歴:
  数学科出身 (修士卒)
  → 社会人 (春から 3 年目)
- 好きな食べ物:
  ラーメン (特に二郎系)

歴史を刻め 大阪 下新庄本店
汁なしラーメン

撮影: ぱい (@END_OF_PAIOTU)

今日話す内容

1. 解析的整数論とは
2. リーマンのゼータ関数 $\zeta(s)$
3. $\zeta(s)$ の仲間 1: ディリクレの L 関数 $L(s,\chi)$
4. $\zeta(s)$ の仲間 2: 多項式環 $\mathbb{F}_p[X]$ のゼータ関数 $\zeta_{\mathbb{F}_p[X]}(s)$
5. まとめ

アンケート

あなたの年代等はどれですか？
(伏せておきたい方は回答しなくて大丈夫です)

1. 中学生・高校生
2. 数学科の大学生・大学院生
3. 数学科以外の大学生・大学院生
4. その他

整数論とは

主に整数の性質を明らかにしようとする分野

→ 特に素数の性質を明らかにしたい！

＜手法＞

- 解析的整数論 → ゼータ関数など複素関数を考察
- 代数的整数論 → 整数係数の代数方程式の解を考察
- 数論幾何 → スキーム論など？（あまり知らない）

1 解析的整数論とは

2 リーマンのゼータ関数 $\zeta(s)$

3 $\zeta(s)$ の仲間 1: ディリクレの L 関数 $L(s,\chi)$

4 $\zeta(s)$ の仲間 2: 多項式環 $\mathbb{F}_p[X]$ のゼータ関数 $\zeta_{\mathbb{F}_p[X]}(s)$

5 まとめ

リーマンのゼータ関数 $\zeta(s)$ とは

定義 1

複素関数 $\zeta(s)$ を

$$\begin{aligned}\zeta(s) &:= \sum_{n\geq 1}\frac{1}{n^s} \quad (s : \text{複素数}, \mathrm{Re}(s) > 1)\\ &= \frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots\end{aligned}$$

で定める．これを「リーマンのゼータ関数」という．

＜解析的整数論の慣習＞

複素変数として，$z = x + y\sqrt{-1}$ の代わりに

$s = \sigma + t\sqrt{-1}$ を用いることが多い．

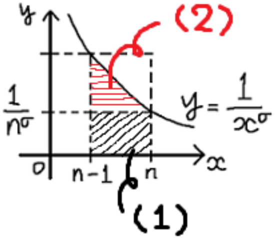
cf. リーマンの論文　独語版 [Ri1], 英訳版 [Ri2].

$\sum_{n\geq 1} n^{-\sigma}$ の収束性 ($\sigma > 1$)

σ:実数とする.

$\sigma > 1$ のとき, $n = N$ までの有限和を評価すると

$$
\begin{aligned}
\sum_{1\leq n\leq N} \frac{1}{n^{\sigma}}
&= 1 + \sum_{1\leq n\leq N} \int_{n-1}^{n} \frac{\mathrm{d}x}{n^{\sigma}} \quad ((1)\text{ の面積}) \\
&< 1 + \sum_{1\leq n\leq N} \int_{n-1}^{n} \frac{\mathrm{d}x}{x^{\sigma}} \quad ((1)+(2)) \\
&= 1 + \int_{1}^{N} \frac{\mathrm{d}x}{x^{\sigma}} \\
&= 1 + \frac{1 - N^{1-\sigma}}{\sigma - 1}.
\end{aligned}
$$



$\sum_{n\geq 1} n^{-\sigma}$ の収束性 $(\sigma > 1)$

$\sigma > 1$ のとき

$$\sum_{1\leq n\leq N} \frac{1}{n^{\sigma}} < 1 + \frac{1 - N^{1-\sigma}}{\sigma - 1}.$$

両辺で $N \to \infty$ とすると, $\sigma > 1$ より

$$\sum_{n\geq 1} \frac{1}{n^{\sigma}} \leq 1 + \frac{1}{\sigma - 1}.$$

よって, $\sigma > 1$ のとき $\sum_{n\geq 1} n^{-\sigma}$ は収束する.

$\sum_{n\geq 1} n^{-\sigma}$ の発散性 ($\sigma \leq 1$)

定理 2

$\sigma \leq 1$ のとき, $\sum_{n\geq 1} n^{-\sigma}$ は発散する.

(証明)

$$
\begin{aligned}
\sum_{n\geq 1} \frac{1}{n^{\sigma}} &\geq \sum_{n\geq 1} \frac{1}{n} \qquad (\sigma \leq 1) \\
&= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \cdots \\
&> 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \cdots \\
&= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots \\
&= \infty
\end{aligned}
$$

$\square$

クイズ1

リーマンの論文 [Ri1] が発表されたのは何年頃でしょうか？

1. 1700 年〜1799 年
2. 1800 年〜1899 年
3. 1900 年〜1999 年

出典: Wikipedia
「ベルンハルト・リーマン」

クイズ1のこたえ

リーマンの論文 [Ri1] が発表されたのは何年頃でしょうか？

こたえ: 2 番 1800 年～1899 年

1700 年代: オイラーが $\zeta(s)$ を研究.

- $\zeta(s)$ の無限積表示や $\zeta(2) = \dfrac{\pi^2}{6}$ などを証明.

1859 年: リーマンが論文 [Ri1] を発表.

- $\zeta(s)$ の積分表示を発見し, $\zeta(s)$ の定義域を拡げた. (解析接続)
- $\mathrm{Re}(s) > 0$ のとき, $\zeta(s) = 0 \Rightarrow \mathrm{Re}(s) = \frac{1}{2}$ だろうと提唱.
  (リーマン予想)

1914 年: ハーディが論文 [H] を発表.

- $\zeta(s) = 0$ かつ $\mathrm{Re}(s) = \frac{1}{2}$ をみたす s が無数に存在することを証明.

$\zeta(s)$ のオイラー積表示

定理 3

$\mathrm{Re}(s) > 1$ のとき, $\zeta(s) = \displaystyle\prod_{p:\text{素数}} \frac{1}{1 - p^{-s}}$ と表せる.

※「$\prod$」は $\sum$ の掛け算バージョン.

		ローマ字	ギリシア文字
和：	*sum*	s, S	σ, Σ
積：	*product*	p, P	π, Π

定理 3 ($\zeta(s)$ のオイラー積表示) の証明

(証明) $$\prod_p \frac{1}{1-p^{-s}}$$

$$= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \quad \text{(等比数列の和)}$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots\right) \times \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right)$$

$$\times \left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \cdots\right) \times \cdots$$

$$= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots + \frac{1}{2^s} + \frac{1}{2^s} \cdot \frac{1}{3^s} + \frac{1}{2^s} \cdot \frac{1}{5^s} + \cdots$$

$$= \sum_{n \geq 1} \frac{1}{n^s} = \zeta(s) \qquad \square$$

素数とリーマン・ゼータ関数 $\zeta(s)$ の関係: その1

定理 4

素数は無限個存在する.

(証明) 背理法で証明する.

定理 3 より,

$$\sum_n \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

もし素数が有限個しか存在しなければ,

$s \to 1$ のとき, 右辺は有限値に収束する.

一方, 定理 2 より, $s \to 1$ のとき, 左辺は発散する.

よって, 素数は無限個存在しなければならない. $\square$

素数とリーマン・ゼータ関数 $\zeta(s)$ の関係: その 2

定理 4

素数は無限個存在する.

(別証明) 背理法で証明する.

定理 3 より,

$$\sum_n \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

もし素数が有限個しか存在しなければ,

$s = 2$ のとき, 右辺の値は有理数となる.

一方, $s = 2$ のとき, 左辺 $= \pi^2/6$ が知られている.

よって, 素数は無限個存在しなければならない. □

(波線部 cf. ぼくのツイート [P])

素数とリーマン・ゼータ関数 $\zeta(s)$ の関係: その 3

関数 $\pi(x)$ を $\pi(x) := \#\{p : \text{素数} \mid p \leq x\}$ とおく.

$s \to 1$ のときの $\zeta(s)$ の振る舞いをさらに深く調べることで,

以下の定理 5 が証明できる.

定理 5 (素数定理)

$\pi(x)$ の極限について,

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \log x} = 1$$

が成り立つ.

cf. 素数定理の入門書 [C]

休　　憩

$\zeta(s)$ の仲間その 1: ディリクレ級数 $L(s,\chi)$

- ディリクレ指標 $\chi(n)$ を定義して,
  $\chi(n)$ に関するディリクレ L 級数 $L(s,\chi)$ を定義する.
- $L(s,\chi)$ と素数の関係を説明する.

ディリクレ指標とは

定義 6

N: 正整数とする. 数列 $\chi(n)$ が「$\bmod N$ のディリクレ指標」であるとは, 以下の 4 つの条件が成り立つときをいう,

$$\begin{aligned}
&(1) \quad \chi(n) \neq 0 \quad (\gcd(n, N) = 1 \text{ のとき}),\\
&(2) \quad \chi(n) = 0 \quad (\gcd(n, N) > 1 \text{ のとき}),\\
&(3) \quad \chi(mn) = \chi(m)\chi(n) \quad (\forall m, n),\\
&(4) \quad m \equiv n \bmod N \ \Rightarrow \ \chi(m) = \chi(n) \quad (\forall m, n).
\end{aligned}$$

例. 以下の χ は mod4 のディリクレ指標となる.

$$\chi(n) = \begin{cases} 1 & (n \equiv 1 \mod 4 \text{ のとき}),\\ -1 & (n \equiv -1 \mod 4 \text{ のとき}),\\ 0 & (n \equiv 0, 2 \mod 4 \text{ のとき}). \end{cases}$$

ディリクレの L 級数 $L(s,\chi)$ とは

定義 7

N: 正整数とする. $\chi(n)$: $\bmod N$ のディリクレ指標とする.
関数 $L(s,\chi)$ を

$$L(s,\chi) := \sum_{n\geq 1} \frac{\chi(n)}{n^s} \quad (\mathrm{Re}(s) : \text{十分大})$$

で定める. これを「χ に関するディリクレの L 級数」という.

素数とディリクレ・L 級数の関係

$s \to 1$ のときの $L(s, \chi)$ の極限について考察することで,
以下の定理 8 が証明できる.

定理 8 (算術級数定理)

N, n:互いに素な正整数とする.
このとき, $p \equiv n \mod N$ であるような素数は無限個存在する.

cf. ザギエの本 [Z]

$\zeta(s)$ の仲間その 2: 多項式環のゼータ

- 有限体 $\mathbb{F}_p$ とその上の多項式環 $\mathbb{F}_p[X]$ を定義して, $\mathbb{F}_p[X]$ のゼータ関数 $\zeta_{\mathbb{F}_p[X]}(s)$ を定義する.
- $\zeta_{\mathbb{F}_p[X]}(s)$ と素数っぽい概念との関係を説明する.

有限体 $\mathbb{F}_p$ とその上の多項式環 $\mathbb{F}_p[X]$ とは

定義 9

p:素数とする．集合 $\mathbb{F}_p$ を

$$\mathbb{F}_p := \{\bmod p \text{ での整数全体}\} = \{0,\ 1,\ 2,\ \ldots,\ p-1\}$$

で定める．これを「位数 p の有限体」とか「p 元体」という．

定義 10

p:素数, $\mathbb{F}_p$: p 元体とする．集合 $\mathbb{F}_p[X]$ を

$$\mathbb{F}_p[X] := \{\mathbb{F}_p \text{係数の多項式全体}\}$$

で定める．これを「$\mathbb{F}_p$ 上の多項式環」という．

多項式環における諸概念その1

定義 11

p:素数とし,
$F(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{F}_p[X]$ とする.
$F(X)$ が「モニックである」とは, $F(X)$ の最高次の係数が $a_d = 1$ のときをいう.

例. $X^2 + 2X + 3$ はモニックである.

例. $p \neq 2$ のとき, $3X^2 + 2X + 1$ はモニックでない.

多項式環における諸概念その 2

定義 12

p:素数とし, $F(X) \in \mathbb{F}_p[X]$ とする.

- $F(X)$ が「可約である」とは,
  定数でないある多項式 $G(X), H(X) \in \mathbb{F}_p[X]$ を用いて
  $F(X) = G(X)H(X)$ と表せるときをいう.
- $F(X)$ が「既約である」とは,
  $F(X)$ が可約でないときをいう.

※モニックな既約多項式は素数と似ている.

(因数分解 $\longleftrightarrow$ 素因数分解)

クイズ 2: $\mathbb{F}_p[X]$ の既約多項式・可約多項式の例

$p = 3$ とする.

$\mathbb{F}_3[X]$ において, 以下の多項式 $F(X)$ は

可約でしょうか？それとも既約でしょうか？

$$F(X) = X^2 + X + 1$$

1. 可約.
2. 既約.

クイズ2のこたえ

$p = 3$ とする.

$\mathbb{F}_3[X]$ において, 以下の多項式 $F(X)$ は

可約でしょうか？それとも既約でしょうか？

$$F(X) = X^2 + X + 1$$

こたえ: 1 番 可約.

- $\mathbb{F}_3$ において, $1 \equiv 4 \bmod p$ である.
  よって,
  $$F(X) = X^2 + X + 1 = X^2 + 4X + 4 = (X + 2)^2$$
  と因数分解できる.
- なお, 通常の整数の範囲では $F(X)$ は既約である.

多項式環 $\mathbb{F}_p[X]$ のゼータ関数 $\zeta_{\mathbb{F}_p[X]}(s)$ とは

定義 13

p:素数とする．数列 $a_p(n)$ を以下で定める．

$$a_p(n) := \begin{cases} \#\left\{F(X) \in \mathbb{F}_p[X] \;\middle|\; \begin{array}{l} F(X)\text{:モニック}, \\ F(X) \text{ の次数は } d \end{array}\right\} & (\exists d, n = p^d), \\ 0 & (\text{その他}). \end{cases}$$

関数 $\zeta_{\mathbb{F}_p[X]}(s)$ を

$$\zeta_{\mathbb{F}_p[X]}(s) := \sum_{n \geq 1} \frac{a_p(n)}{n^s} \quad (\mathrm{Re}(s) : \text{十分大})$$

で定める．これを「$\mathbb{F}_p[X]$ のゼータ関数」という．

整理すると，$\zeta_{\mathbb{F}_p[X]}(s) = \displaystyle\sum_{F\text{:モニック}} \frac{1}{\left(p^{\deg F(X)}\right)^s}$ と表せる．

$\zeta_{\mathbb{F}_p[X]}(s)$ のオイラー積表示

多項式 $F(X)$ の因数分解を考えることで,

以下の定理 14 が分かる.

定理 14

p:素数とする.
$\mathbb{F}_p[X]$ のゼータ関数 $\zeta_{\mathbb{F}_p[X]}(s)$ は以下のオイラー積を持つ.

$$\begin{aligned}\zeta_{\mathbb{F}_p[X]}(s) &= \sum_{F(X):\text{モニック}} \frac{1}{\left(p^{\deg F(X)}\right)^s} \\ &= \prod_{\substack{P(X):\text{モニック}\\ \text{かつ既約}}} \frac{1}{1-\left(p^{\deg P(X)}\right)^{-s}}.\end{aligned}$$

$\mathbb{F}_p[X]$ 版の素数定理

p:素数, d:正整数とする．関数 $\varpi_p(d)$ を

$$\varpi_p(d) := \#\left\{ P(X) \in \mathbb{F}_p[X] \;\middle|\; \begin{array}{c} P(X)\text{:モニックかつ既約,} \\ P(X)\text{ の次数は } d \end{array} \right\}$$

で定める．

※「ϖ」は「π」の異字体.

LaTeX のコマンドで「¥varpi」と入力すれば出てくる.

$\mathbb{F}_p[X]$ 版の素数定理

p:素数, d:正整数とする. 関数 $\varpi_p(d)$ を

$$\varpi_p(d) := \#\left\{P(X) \in \mathbb{F}_p[X] \;\middle|\; \substack{F(X):\text{モニックかつ既約},\\ \deg P(X)=d}\right\}$$

で定める.

$\zeta_{\mathbb{F}_p[X]}(s)$ をオイラー積表示してから微分を考えることで, 以下の定理 15 が証明できる.

定理 15

p:素数, d:正整数, $x = p^d$ とする. このとき,

$$\lim_{d\to\infty} \frac{\varpi_p(d)}{p^d/d} = \lim_{x\to\infty} \frac{\varpi_p(d)}{x/\log x} = 1$$

が成り立つ.

cf. 多項式環上の整数論の解説書 [Ro]

ディリクレ級数 ($\neq$ ディリクレの L 級数)

定義 16

一般に, 数列 $a(n)$ を用いて以下の形で表される級数を「ディリクレ級数」という.

$$\sum_{n\geq 1} \frac{a(n)}{n^s}.$$

ディリクレ級数のうち, 整数論的に面白いものを

「ゼータ関数」や「L 関数」と呼ぶ.

ディリクレ級数の性質

定理 17

$a(n)$ を数列とする．このとき，次の 2 つが成り立つ．

- $\exists \sigma_0 \in \mathbb{R} \cup \{\pm\infty\}$ s.t.
$$\mathrm{Re}(s) > \sigma_0 \implies \sum_{n \geq 1} \frac{a(n)}{n^s} \text{ は収束.}$$
- $a(mn) = a(m)a(n)\ (\forall\, m, n)$
$$\implies \sum_{n \geq 1} \frac{a(n)}{n^s} = \prod_p \left(\sum_{r \geq 0} \frac{a(p^r)}{p^{rs}} \right).$$

cf. ディリクレ級数の参考書 [M]

まとめ

ゼータ		相性のいい対象
$\zeta(s)$	$\longleftrightarrow$	一般の素数
$L(s,\chi)$	$\longleftrightarrow$	$p \equiv n \mod N$ の形の素数
$\zeta_{\mathbb{F}_p[X]}(s)$	$\longleftrightarrow$	モニックな既約多項式

ゼータ関数は他にもたくさんある.

君のお気に入りのゼータを探してみよう！

参考文献

[C] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Springer (1968).

[H] G. H. Hardy, *Sur les Zeros de la Fonction* $\zeta(s)$ *de Riemann*, Acad. Sci. Paris, **158**, pp. 1012-1014 (1914).

[M] S. Mandelbrojt, *Dirichlet Series: Principles and Methods*, D. Reidel Publishing Company (1972).

[P] ぱい (@END_OF_PAIOTU), *https://twitter.com/END_OF_PAIOTU/ status /1472489925027438594?s=20&t=O8sP3jqNxI4iz9gnaIHETA* (2021 年 12 月 19 日のツイート).

[Ri1] B. Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grotsse*, Monatsb. Preuss. Akad. Wiss. Nov. pp.671-680 (1859).

[Ri2] B. Riemann (著), R. Baker, Ch. Christenson, and H. Orde (英訳), *Bernhard Riemann: Collected Papers, paper VII*, Kendrick Press, pp.135-143 (2004)).

[Ro] M. Rosen, *Number Theory in Function Fields*, Springer (2000).

[Z] Don B. Zagier (著), 片山孝次 (和訳), 数論入門: ゼータ関数と 2 次体, 岩波書店 (1990).