

# 算術級数の素数定理

高校3年3組22番 清水元喜

## 1 はじめに

今日は数学研究部にお越しいただきありがとうございます。はじめにこの記事で扱う内容について少し解説します。

去年、僕はこの部誌で「 $\mathbb{Z}[i]$ における算術級数定理」を示しました。そこで最初、今年「 $\mathbb{Z}[i]$ における素数定理」を示そうと思いましたが、すぐにわかることですがこれは、

$$\pi_{4,1}(x) \sim \pi_{4,3}(x) \sim \frac{1}{2} \frac{x}{\log x} (x \rightarrow \infty)$$

に帰着されます。

また、たまたま読んでいた数学書たちにぼそっと、「実は、

$$\pi_{m,a}(x) \sim \frac{1}{\phi(m)} \frac{x}{\log x}$$

である。」と書かれていたのですが、証明は載っていませんでした。そこで今回これを示すことにしました。つまり、

**定理 1.1** (算術級数中の素数定理).  $\pi(x)$  を  $x$  以下の素数の個数とし、また  $(a, m) = 1$  のとき  $\pi_{m,a}(x)$  を  $x$  以下の素数で  $\text{mod } m$  で  $a$  に合同なものの素数とする。<sup>1</sup>このとき、

$$\pi_{m,a}(x) \sim \frac{1}{\phi(m)} \pi(x) \sim \frac{1}{\phi(m)} \frac{x}{\log x}$$

である。ここで  $\phi(m)$  は  $m$  の既約剰余類の個数、 $f(x) \sim g(x)$  ( $x \rightarrow \alpha$ ) は  $\lim_{x \rightarrow \alpha} f(x)/g(x) = 1$  を意味します。

この定理から、「素数は  $\text{mod } m$  で均等に分布している」ことがわかります。(去年、算術級数定理を示したときにも同じようなことを書きましたが。)

---

<sup>1</sup>別に  $(a, m) > 1$  の時にも  $\pi_{m,a}(x)$  は定義は出来ませんが、まったく意味のない関数ですし、今後いちいち  $(a, m) = 1$  と断るのが面倒なのでこう書きました。

## 2 準備

### 2.1 解析

**定理 2.1** (Cauchy の判定法). 数列  $\{a_n\}$  が収束する必要十分条件は、任意の  $\epsilon > 0$  に対してある  $n_0$  があって、

$$p > n_0, q > n_0 \Rightarrow |a_p - a_q| < \epsilon$$

となることである。

**定義 2.2** (無限級数とその収束). 数列  $\{a_n\}$  に対して、

$$s_n = a_1 + a_2 + \dots + a_n$$

とする。もしも (有限の) 極限值

$$\lim_{n \rightarrow \infty} s_n = s$$

が存在するならば、無限級数

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \dots + a_n + \dots$$

は収束するといひ、極限  $s$  をこの無限級数の和と略称する。極限值が存在しないとき ( $\lim s_n = \pm\infty$  をも含めていう) には無限級数は発散するという。

Cauchy の判定法 (定理 2.1) に収束の必要十分条件は、任意の  $\epsilon > 0$  に対して

$$R_{n,m} = s_m - s_n = a_{n+1} + a_{n+2} + \dots + a_m$$

とおくと必ずある番号以上で  $|R_{n,m}| < \epsilon$  と出来ることである。

**定義 2.3** (絶対収束、条件収束). 無限級数  $\sum a_n$  の絶対値の級数  $\sum |a_n|$  が収束するときには、原級数  $\sum a_n$  も収束する。実際

$$|R_{n,m}| = |a_{n+1} + a_{n+2} + \dots + a_m| \leq |a_{n+1}| + |a_{n+2}| + \dots + |a_m|$$

で、仮定によって、右辺は  $n \rightarrow \infty$  のとき、限りなく小さくなるから、左辺も同様である。この場合に、級数  $\sum a_n$  は絶対収束をするという。

級数が収束して、しかも絶対収束をしないときは、それを条件収束という。

絶対収束の級数は項を勝手に並び替えてよいなどおおむね有限和と同様の性質を持つ。

**定義 2.4** (一様収束). 或る区間に属する各点  $x$  において、関数の列

$$f_1(x), f_2(x), \dots, f_n(x), \dots$$

が収束するときには、その極限はその区間における  $x$  の関数である。それを  $f(x)$  とする。もしも任意の  $\epsilon > 0$  に対応して、或る番号  $n_0$  が定められて、

$$n > n_0, x \in [a, b] \text{ なるとき、常に } |f(x) - f_n(x)| < \epsilon$$

すなわち収束の速さが  $x$  によらずに評価できるときに関数列  $\{f_n(x)\}$  は  $[a, b]$  において一様に (または平等に)  $f(x)$  に収束するという。

無限級数の項  $a_n = a_n(x)$  が  $x$  の関数である場合に、或る区間において  $s_n(x) = \sum_{v=1}^n a_v(x)$  が一様に収束するとき、この級数を一様に収束するという。この場合  $s_n(x) \rightarrow s(x)$  として

$$s(x) - s_n(x) = \sum_{v=n+1}^{\infty} a_v(x) = R_n(x)$$

と置けば、 $R_n(x)$  は一様に 0 に収束する。

級数の一様収束は、しばしば、次の定理によって確かめられる。

**定理 2.5.** 或る区間において常に  $|a_n(x)| \leq c_n$ ,  $c_n$  は正の定数で、 $\sum_{n=1}^{\infty} c_n$  が収束すれば、級数  $\sum_{n=1}^{\infty} a_n(x)$  はその区間において絶対一様収束する。

**定義 2.6.**  $\frac{f(x)}{g(x)}$  が有界であるときに  $f(x) = O(g(x))$  と書く。また、 $\frac{f(x)}{g(x)} \rightarrow 0$  (何も断らない場合  $x \rightarrow \infty$ , 他の値への極限をとることも当然ある) であるときに、 $f(x) = o(g(x))$  と書く。また、 $\frac{f(x)}{g(x)} \rightarrow 1$  (同上) であるときに、 $f(x) \sim g(x)$  と書く。<sup>2</sup>

### 2.1.1 複素解析

**定義 2.7** (位相の用語).  $U \subset \mathbb{C}$  が開集合であるとは、任意の  $a \in U$  に対してある  $\epsilon > 0$  が存在して、

$$|z - a| < \epsilon \Rightarrow z \in U$$

---

<sup>2</sup>~については前書きで少し触れましたが、大事なことなので二回言いました。

が成り立つことを言う。 $a$  を含む開集合を  $a$  の開近傍といい、 $a$  のある開近傍を含む集合を  $a$  の近傍という。

補集合が開集合であるような集合を閉集合という。有界な閉集合をコンパクト集合という。

**命題 2.8.**  $f$  が開集合  $U$  上で連続  $\Rightarrow |f|$  は  $U$  上の任意のコンパクト集合上で最大値を持つ

$\mathbb{C}$  においても、絶対収束/条件収束、一様収束などの概念は同様に定義される。

**定義 2.9** (正則関数). 開集合  $U$  上で定義された複素微分可能な関数を  $U$  上の正則関数という。 $f$  が正則であることは、定義域内の任意の  $a$  の近傍で

$$f(z) = a_0 + a_1(z - a) + a_2(z - a)^2 + \dots$$

と *Taylor* 展開できることと同値である。(「複素微分可能」の条件を述べるのはやや複雑なので知らない人は「*Taylor* 展開が可能」ということだと思っておいてください。)

**命題 2.10** (一致の原理). 正則関数  $f, g$  があってある点の近傍で  $f = g \Rightarrow$  定義域全体で  $f = g$

**命題 2.11.** 領域  $\{z \in \mathbb{C} | r < |z - a| < R\}$  上の正則関数  $f$  に対して無限級数表示

$$f(z) = \sum_{-\infty}^{\infty} a_n(z - a)^n$$

ができる。これを *Laurent* 展開と呼ぶ。

**定義 2.12** (特異点). 正則関数が  $a$  の近傍で定義されており  $a$  では定義されていないとし、前命題の *Laurent* 展開を考える。 $a_{-n} \neq 0$  なる整数  $n$  に上界が存在しないとき、 $a$  を真性特異点という。そうでないとき、 $a_{-n} \neq 0$  なる整数  $n$  の最大値を  $m$  とし、次のように定義する。

- $m \leq 0$  のとき  $f$  を正則に拡張して  $a$  を定義域に付け加えることができる。このような  $a$  を除去可能特異点という。
- $m > 0$  のとき、 $a$  を  $m$  位の極という。

開集合  $U$  上の、極を除いて定義された正則関数を  $U$  上の有理型関数という。

**定義 2.13** (留数). 有理型関数の極に対して、留数という値が定義される。 $z = z_0$  を極にもつ有理型関数  $f(z)$  が与えられたとき、 $f$  の  $z = z_0$  の周りでの *Laurent* 展開の  $\frac{1}{z - z_0}$  の係数  $a_{-1}$  を  $f$  の  $z = z_0$  での留数と呼び、 $\text{Res}_{z=z_0} f(z) = a_{-1}$  と書く。とくに  $z = z_0$  が 1 位の極であるとき、明らかに

$$\text{Res}_{z=z_0} f(z) = \lim_{z \rightarrow z_0} \{(z - z_0)f(z)\}$$

**命題 2.14.**  $f, g$  が正則関数  $\Rightarrow f \pm g, fg, f^{-1}$  はそれぞれ正則 (いずれも演算が定義されるとき) また、 $f, g$  が有理型関数で  $g$  が恒等的に 0 でないならば有理型関数  $f/g$  が自然に定義できる。

**命題 2.15.**<sup>3</sup>

$f_1, f_2, \dots$  を正則関数列とし、これが  $U$  上の任意のコンパクト集合上で  $f$  に一様収束しているならば、 $f$  は正則関数であり、

$$f'(z) = \lim_{n \rightarrow \infty} f'_n(z)$$

**定義 2.16** (解析接続). 2つの領域  $D_1, D_2$  が共通部分を持つとする。 $f_1(z)$  が  $D_1$  で正則な (もしくは有理型) 関数であるとき、 $D_1 \cap D_2$  で  $f_1(z)$  と同じ値をとり、しかも  $D_2$  で正則な (もしくは有理型) 関数  $f_2(z)$  が存在する場合、 $f_2(z)$  を  $f_1(z)$  の  $D_2$  への解析接続であるという。命題 2.10 (一致の原理) より、 $D_2$  への解析接続は一意的に定まる。

例.

$$f_1(z) = \sum_{n=0}^{\infty} z^n$$

は  $|z| < 1$  で収束、 $|z| \geq 1$  で発散するから、 $|z| < 1$  でのみ定義される関数で、

$$f_1(z) = \frac{1}{1-z} (|z| < 1)$$

である。一方、関数

$$f_2(z) = \frac{1}{1-z} (z \neq 1)$$

は  $\mathbb{C} - \{1\}$  で定義される正則関数である。今 2 つの関数の定義域の共通部分  $|z| < 1$  で  $f_1 = f_2$  であるから、 $f_2$  は  $f_1$  の  $z = 1$  を除く  $\mathbb{C}$  上への解析接続である。

<sup>3</sup>この命題、結構あとで使います。重要です。

## 2.2 指標

**定義 2.17** (Abel 群). 集合  $G$  について、演算  $+: G \times G \rightarrow G$  が定められており、 $G$  の任意の元  $a, b, c$  について以下の (G1)~(G4) が成り立つとき、 $G$  は Abel 群 (加群) であるという。

**G1**  $a + b = b + a$

**G2**  $a + (b + c) = (a + b) + c$

**G3**  $G$  の元  $e$  で任意の  $G$  の元  $a$  について  $a + e = e + a = a$  を満たすものがある

**G4** 任意の  $G$  の元  $b$  について  $b + (-b) = (-b) + b = e$  を満たすような  $G$  の元  $(-b)$  が存在する

以下  $G$  を有限 Abel 群とします。

**定義 2.18** (位数).  $G$  の元の個数を  $G$  の位数と呼び、 $\text{card}(G)$  と書く。

**定義 2.19** (指標).  $G$  の指標とは、 $G$  から  $\mathbb{C}^*$  への写像  $\chi$  で、任意の  $G$  の元  $a, b$  に対し  $\chi(ab) = \chi(a)\chi(b)$  を満たすものである。 $G$  の指標全体の集合を  $\hat{G}$  であらわす。

**命題 2.20.**  $\chi$  を指標とすると  $|\chi(a)| = 1$

これは  $a^{\text{card}(G)} = e$  (単位元) より分かります。

**命題 2.21.**  $\chi(a^{-1}) = \overline{\chi(a)} = \bar{\chi}(a)$

**命題 2.22** (指標群).  $\chi_1, \chi_2 \in \hat{G}$  について  $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$  と定義することで  $\hat{G}$  はこの演算について Abel 群となる。これを  $G$  の指標群と呼ぶ。また、以下でこの群の単位元 (すなわち全ての元を 1 に移す指標: 単位指標とも言う) を誤解の恐れのないときは 1 と書くことがある。

**命題 2.23.**  $H$  を  $G$  の部分群とする。このとき  $H$  の指標は  $G$  での指標に拡張することができる。

**命題 2.24.**  $\text{card}(G) = \text{card}(\hat{G})$

**命題 2.25.**  $n = \text{card}(G), \chi \in \hat{G}$  とすると、

$$\sum_{a \in G} \chi(a) = \begin{cases} n & (\chi = 1) \\ 0 & (\chi \neq 1) \end{cases}$$

**命題 2.26.**  $n = \text{card}(G), a \in G$  とすると、

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} n & (a = 1) \\ 0 & (a \neq 1) \end{cases}$$

また、特に  $G$  として  $(\mathbb{Z}/m\mathbb{Z})^*$  を考えるとき、 $(a, m) > 1$  なる  $a$  について  $\chi(a) = 0$  と定めることで  $\chi$  を  $\mathbb{Z} \rightarrow \mathbb{C}$  なる写像だとみなすことができる。これを  $\text{mod } m$  の指標と呼ぶ。というか、今後こいつしか出てきません。以下、 $\chi(n)$  とでてきたらそれは基本的に  $\text{mod } m$  の指標です。<sup>4</sup>

## 2.3 整数論

初等整数論の基本的な知識は既知のものとしします。分からない箇所があったら、[2]などを参照してみてください。また、僕の去年の記事にも一応まとめてあります。そんなに多くの整数論的知識は仮定しません。

あ、あとどこに書くべきか微妙な注意なのでここに書いておくと、今後でてくる  $p$  という文字は素数を表します。あと変数  $s, z$  は複素数であることがほとんどだと思います。 $n$  とか  $m$  とか  $a$  とかは多分自然数や整数をあらわすはずです。文字がどの範囲は基本的に書きますが慣例上もしくは文脈上明らかな場合はしばしば省略しますので大目に見てください。

## 3 まずは素数定理

方針としては、まず素数定理を示してから、それと同様の方法で示すことを考えます。素数定理の証明方法はいくつも知られていますが、今回は[1]の方針に従います。

**定義 3.1.** 関数  $\zeta(s), \Phi(s), \theta(x)$  を、

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \Phi(s) = \sum_p \frac{\log p}{p^s}, \theta(x) = \sum_{p \leq x} \log p \quad (s \in \mathbb{C}, x \in \mathbb{R})$$

として定義する。

**命題 3.2 (Euler 積).**  $\zeta(s) = \prod_p (1 - p^{-s})^{-1} (\text{Re}(s) > 1)$

---

<sup>4</sup>だったらその場合に限った定義、説明だけすればよかったですね。決して去年のをそのままコピペして修正したくなくなったからとかではないです。

**証明.** これは有名ですし、証明は省略します。(去年の僕の部誌に一応証明は載っています) □

**命題 3.3** (解析接続).  $\zeta(s) - \frac{1}{s-1}$  は  $\operatorname{Re}(s) > 0$  に正則に解析接続される。

**証明.**

$$\frac{1}{s-1} = \int_1^\infty t^{-s} dt = \sum_{n=1}^\infty \int_n^{n+1} t^{-s} dt \text{ より、}$$

$\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt$  とおき、 $\phi(s) = \sum_{n=1}^\infty \phi_n(s)$  が  $\operatorname{Re}(s) > 0$  で正則であることをいえばよい。今各  $\phi_n(s)$  が  $\operatorname{Re}(s) > 0$  で正則なのは明らかで、正則関数の一様収束による収束先はまた正則だから、 $\sum_{n=1}^k \phi_n(s)$  が  $\operatorname{Re}(s) > 0$  上の任意のコンパクト集合上で一様収束することを示せばよい。

$$\begin{aligned} |\phi_n(s)| &\leq \int_n^{n+1} |n^{-s} - t^{-s}| dt \\ &\leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}| \end{aligned}$$

ところで今、

$$\begin{aligned} |n^{-s} - t^{-s}| &= \left| \int_n^t \frac{s}{t^{s+1}} dt \right| \\ &\leq \int_n^t \left| \frac{s}{t^{s+1}} \right| dt \\ &= |s| \int_n^t \frac{dt}{t^{x+1}} \quad (x = \operatorname{Re}(s)) \\ &\leq \frac{|s|}{n^{x+1}} \end{aligned}$$

より、 $\phi_n(s) \leq \frac{|s|}{n^{x+1}}$ 。今  $S$  を  $\operatorname{Re}(s) > 0$  上のコンパクト集合とすると、 $s \in S$  に対し  $|s|$ 、 $\operatorname{Re}(s)$  にはそれぞれ最大値と最小値が存在するからそれを  $M, m$  とすると、 $S$  上で  $|\phi_n(s)| \leq \frac{M}{n^{m+1}}$  定理 2.5 より、 $\sum_{n=1}^k \phi_n(s)$  はこのコンパクト集合上で絶対一様収束する。ゆえに  $\phi(s)$  は  $\operatorname{Re}(s) > 0$  で正則。 □

**命題 3.4.**  $\theta(x) = O(x)$

**証明.**  $n \in \mathbb{N}$  に対して、

$$2^{2n} = (1+1)^{2n} \geq \binom{2n}{n} \geq \prod_{n < p \leq 2n} p = e^{\theta(2n) - \theta(n)}$$

ここで最初の不等号は二項定理より、次の不等号は  $n < p \leq 2n$  を満たす  $p$  について明らかに  $p \mid \binom{2n}{n} = (2n)!/(n!)^2$  であることから従います。ここから、 $2n \log 2 \geq \theta(2n) - \theta(n)$  がわかります。また、 $\theta(x)$  は  $x$  が 1 増えるとき高々  $\log x$  しか増加しないことに注意してこの関係を使うと、

$$\begin{aligned} \theta(2x) - \theta(x) &= \theta(\lfloor 2x \rfloor) - \theta(\lfloor x \rfloor) \\ &\leq \theta(2\lfloor x \rfloor + 1) - \theta(\lfloor x \rfloor) \\ &\leq \theta(2\lfloor x \rfloor) + \log(2\lfloor x \rfloor + 1) - \theta(\lfloor x \rfloor) \\ &\leq 2\lfloor x \rfloor \log 2 + \log(2x + 1) \\ &\leq 2x \log 2 + \log(2x + 1) \end{aligned}$$

よって  $C > 2 \log 2$  を任意に取ったとき、ある定数  $x_0 = x_0(C)$  があって任意の  $x > x_0$  について  $\theta(2x) - \theta(x) \leq Cx$  が成立する。今  $x/2^{r+1} < x_0 \leq x/2^r$  なる  $r$  を選んで  $x, x/2, x/4, \dots, x/2^r$  について和をとることで、 $\theta(x) < 2Cx + \theta(x_0)$  がわかり、 $\theta(x) = O(x)$  が示された。□

**命題 3.5** ( $\zeta$  の零点).  $\zeta(s) \neq 0$  ( $\operatorname{Re}(s) \geq 1$ ) で、この範囲で  $\Phi(s) - \frac{1}{s-1}$  は正則。

**証明.**  $\sigma > 1$  とする。このとき Euler 積表示より、

$$\begin{aligned} \log |\zeta(\sigma + it)| &= \frac{1}{2} \left( \log \zeta(s) + \log \overline{\zeta(s)} \right) \\ &= -\frac{1}{2} \sum_p (\log(1 - p^{-s}) + \log(1 - p^{-\bar{s}})) \\ &= \frac{1}{2} \sum_p (p^{-s} + \frac{1}{2} p^{-2s} + \frac{1}{3} p^{-3s} + \dots + p^{-s} + \frac{1}{2} p^{-2\bar{s}} + \dots) \\ &= \sum_p (\operatorname{Re}(p^{-s}) + \frac{1}{2} \operatorname{Re}(p^{-2s}) + \dots) \\ &= \sum_p \sum_{k=1}^{\infty} \frac{1}{k p^{k\sigma}} \cos(kt \log p) \end{aligned}$$

である。今 Euler 積表示より  $\operatorname{Re}(s) > 1$  には明らかに零点はない。 $\zeta(1+it) = 0$  として矛盾を導く。

$$\begin{aligned}
& \log |\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it)| \\
&= \sum_{k,p} \frac{1}{kp^{k\sigma}} (3 + 4 \cos(kt \log p) + \cos(2kt \log p)) \\
&= 2 \sum_{k,p} \frac{1}{kp^{k\sigma}} (1 + \cos(kt \log p))^2 \geq 0
\end{aligned}$$

よって、

$$|\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it)| \geq 1$$

一方、 $\sigma \rightarrow 1$ の時、

$$\zeta(\sigma)^3 = O\left(\frac{1}{(\sigma - 1)^3}\right)$$

$$\zeta(\sigma + it)^4 = O((\sigma - 1)^4)$$

$$\zeta(\sigma + 2it) = O(1)$$

よって、 $\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it) \rightarrow 0$  ( $\sigma \rightarrow 1$ ) となり矛盾。

次に  $\Phi(s)$  についての主張を示す。Euler 積表示で対数をとって微分することで、

$$-\frac{\zeta'}{\zeta}(s) = \sum_p \frac{\log p}{p^s - 1} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)}$$

ここで、右辺第二項は  $\operatorname{Re}(s) > 1/2$  で絶対一様収束し正則。したがって  $\Phi(s)$  は  $s = 1$  及び  $\zeta(s)$  の零点でのみ極を持つことになるが  $\operatorname{Re}(s) \geq 1$  について  $\zeta(s)$  は零点を持たない。 $s = 1$  での留数を調べる。 $\zeta(s) - 1/(s - 1) = \phi(s)$  とおく。 $\phi(s)$  は  $\operatorname{Re}(s) \geq 1$  で正則。

$$\frac{\zeta'}{\zeta}(s) = \frac{\phi'(s) - (s - 1)^{-2}}{\phi(s) + (s - 1)^{-1}} \sim \frac{-1}{s - 1} \quad (s \rightarrow 1)$$

よって  $s = 1$  での留数は 1 となり、主張が従う。 □

**命題 3.6.**  $\int_1^\infty \frac{\theta(x) - x}{x^2} dx$  は収束する。

**証明.**  $\operatorname{Re}(s) > 1$  に対して、

$$\Phi(s) = \sum_p \frac{\log p}{p^s} = \int_1^\infty \frac{d\theta(x)}{x^s} = s \int_1^\infty \frac{\theta(x)}{x^{s+1}} dx = s \int_0^\infty e^{-st} \theta(e^t) dt$$

ここで、第二項は Stieltjes 積分<sup>5</sup> というものであり、これをご存知の方なら、第三項は  $\theta(x)$  と  $\Phi(s)$  の定義より明らか、また第四項は部分積分すれば直ちに従う。と書けばわかってくれるでしょう。Stieltjes 積分を知らない人のために第四項を第一項より直接導いておきます。

$$\begin{aligned} s \int_1^\infty \frac{\theta(x)}{x^{s+1}} dx &= \sum_{k=1}^\infty \int_{p_k}^{p_{k+1}} \frac{s}{x^{s+1}} \theta(p_k) dx \quad (\text{ここで } p_k \text{ は } k \text{ 番目の素数}) \\ &= \sum_{k=1}^\infty \theta(p_k) \left( \frac{1}{p_k^s} - \frac{1}{p_{k+1}^s} \right) \\ &= \sum_{k=1}^\infty \frac{(\theta(p_k) - \theta(p_{k-1}))}{p_k^s} \quad (\text{ここで } p_0 = 1 \text{ とすればよい}) \\ &= \sum_{k=1}^\infty \frac{\log p_k}{p_k^s} = \Phi(s) \end{aligned}$$

ここで、わざわざ第五項のような変な?形に積分を最終的に変形したのは次の補題を使うためです。

**補題 3.7.**  $f(t)$  は  $t \geq 0$  で有界かつ局所的に積分可能とする。(つまり、任意の  $a, b \in \mathbb{R}$  について  $\int_a^b f(t) dt$  が存在するとする。) また、 $g(z) = \int_0^\infty f(t) e^{-zt} dt$  ( $\operatorname{Re}(z) > 0$ ) が  $\operatorname{Re}(z) \geq 0$  に正則に解析接続されるとする。このとき、 $\int_0^\infty f(t) dt$  は存在して  $g(0)$  に等しい。

この補題の証明は複素関数論の知識をそこそこ使うことと、僕の体力の限界から割愛します。[1] を参照してください。

$f(t) = \theta(e^t) e^{-t} - 1$ ,  $g(z) = \Phi(z+1)/(z+1) - 1/z$  としてこの補題を使います。まず、 $f(t)$  が条件を満たすことは命題 3.4 から明らかです。また、 $g(z) = (\Phi(z+1) - 1/z - 1)/(z+1)$  なので、命題 3.5 より、これは  $\operatorname{Re}(z) \geq 0$  で正則です。また、 $g(z) = \int_0^\infty f(t) e^{-zt} dt$  となっていることは計算すれば明らかです。したがって、 $\int_0^\infty f(t) dt = \int_1^\infty \frac{\theta(x) - x}{x^2} dx$  は存在することがわかりました。□

**命題 3.8.**  $\theta(x) \sim x$

**証明.** まあ  $\theta(x)$  の大きさの位数が 1 より小さくても大きくても命題 3.6 は成立しそうにないですよ。証明になってませんが。

<sup>5</sup> スティルチェスと読みます

まず、 $\theta(x) > \lambda x$  を満たす  $x$  が無限に大きく取れるような  $\lambda > 1$  が存在したとします。このとき、

$$\int_x^{\lambda x} dt \frac{\theta(t) - t}{t^2} dt > \int_x^{\lambda x} \frac{\lambda x - t}{t^2} dt = \lambda - 1 - \log \lambda > 0$$

ここで  $\theta(x)$  が広義単調増加であることを用いました。ところが、命題 3.6 より、 $\int_x^{\lambda x} \frac{\theta(t) - t}{t^2} dt \rightarrow 0 (x \rightarrow \infty)$  とならないといけないので、これは矛盾です。

同様に、 $\theta(x) < \lambda x$  を満たす  $x$  が無限に大きく取れるような  $\lambda < 1$  が存在したとします。すると

$$\int_{\lambda x}^x \frac{\theta(t) - t}{t^2} dt < \int_{\lambda x}^x \frac{\lambda x - t}{t^2} dt = -(\lambda - 1 - \log \lambda) < 0$$

となって同様に矛盾です。

よって  $\theta(x)/x \rightarrow 1 (x \rightarrow \infty)$  がわかりました。

□

ここから素数定理が示されます。

$$\theta(x) = \sum_{p \leq x} \log p \leq x \leq \sum_{p \leq x} \log x = \pi(x) \log x$$

また任意の  $\epsilon > 0$  に対して

$$\begin{aligned} \theta(x) &\geq \sum_{x^{1-\epsilon} \leq p \leq x} \log p \geq \sum_{x^{1-\epsilon} \leq p \leq x} (1 - \epsilon) \log x \\ &= (1 - \epsilon) \log x (\pi(x) + O(x^{1-\epsilon})) \end{aligned}$$

よって、

$$\frac{\theta(x)}{x(1-\epsilon)} + O\left(\frac{x^{1-\epsilon} \log x}{x}\right) \leq \frac{\pi(x) \log x}{x} \leq \frac{\theta(x)}{x}$$

となり、 $x \rightarrow \infty, \epsilon \rightarrow 0$  とすることで素数定理が得られる。

## 4 算術級数の素数定理

定義 4.1.

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \Phi_{m,a}(s) = \sum_{p, \chi} \chi(a)^{-1} \chi(p) \frac{\log p}{p^s}$$

$$\theta_{m,a}(x) = \phi(m) \sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \log p$$

**命題 4.2** (Euler 積).  $L(s, \chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1} (Re(s) > 1)$

**証明略**

**命題 4.3.**  $\chi$  が単位指標でないとき、 $L(s, \chi)$  は  $Re(s) > 0$  で正則、また単位指標のとき、 $s = 1$  のみで 1 位の極を持ち、留数は  $\phi(m)/m$  である。

**証明.**  $\chi$  が単位指標でないとき、 $Re(s) > 0$  での収束について考える。 $f_k(s) = \sum_{n=1}^m \frac{\chi(n)}{(km+n)^s}$  と定義すると、 $L(s, \chi) = f_0(s) + \sum_{k=1}^{\infty} f_k(s)$  である。

$$\begin{aligned} |f_k(s)| &= \left| \sum_{n=1}^m \chi(n) \left( \frac{1}{(km+n)^s} - \frac{1}{(km)^s} \right) \right| \quad (\chi \neq 1 \text{ より } \sum_{n=1}^m \chi(n) = 0) \\ &= \left| \sum_{n=1}^m \chi(n) \left( - \int_{km}^{km+n} \frac{s}{x^{s+1}} dx \right) \right| \\ &\leq \sum_{n=1}^m |\chi(n)| \cdot n \cdot |s| \cdot \left| \frac{1}{(km)^{s+1}} \right| \\ &\leq \sum_{n=1}^m \cdot \frac{|s|}{k^{\sigma+1}} \quad (\text{ここで } Re(s) = \sigma \text{ とおいた}) \\ &= m \cdot \frac{|s|}{k^{\sigma+1}} \end{aligned}$$

ゆえに明らかに  $\sum_{k=1}^{\infty} f_k(s)$  は  $Re(s) > 0$  の範囲内で一様収束し、正則関数列の一様収束による極限は正則なので、しめされた。 $\chi$  が単位指標のときは、 $L(s, \chi)$  の Euler 積表示は、

$$L(s, \chi) = \sum_{(n,m)=1} \frac{1}{n^s} = \zeta(s) \prod_{p|m} (1 - \frac{1}{p^s})$$

留数は  $\zeta(s)$  の  $s = 1$  での留数と、

$$\prod_{p|m} (1 - \frac{1}{p}) = \frac{\phi(m)}{m}$$

よりわかる。 □

**命題 4.4.**  $\theta_{m,a}(x) = O(x)$

**証明.** これは命題 3.4 より明らか。 □

**命題 4.5 (零点).**  $Re(s) \geq 1$  で、 $L(s, \chi) \neq 0$ ,  $\Phi_{m,a}(s) - \frac{1}{s-1}$  は正則。

**証明.** Euler 積表示から、 $L(s, \chi)$  は  $Re(s) > 1$  で零点を持たない。次に、 $L(1+it, \chi) = 0$  とする。このとき、 $\zeta(s)$  の時の証明と同様にして、

$$\log |L(s, \chi)| = \sum_{k,p} \frac{1}{k} Re \left( \left( \frac{\chi(p)}{p^s} \right)^k \right) = \sum_{k,p} \frac{1}{kp^{k\sigma}} \cos(k(-c_p + t \log p))$$

となる。(ここで  $c_p$  は  $\chi_p = e^{ic_p}$  となるようにとる。) 今  $\chi$  が単位指標である時は  $\zeta(s)$  の零点に関する考察から明らかだから  $\chi$  は単位指標ではないとしてよい。

$$\begin{aligned} & \log |L(\sigma, 1)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)| \\ &= \sum_{k,p} \frac{1}{kp^{k\sigma}} (3 + 4 \cos(k(-c_p + t \log p)) + \cos(k(-2c_p + 2t \log p))) \\ &= 2 \sum_{k,p} \frac{1}{kp^{k\sigma}} (1 + \cos(k(-c_p + t \log p)))^2 \geq 0 \end{aligned}$$

よって

$$|L(\sigma, 1)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)| \geq 1$$

一方、 $\sigma \rightarrow 1$  の時、 $|L(\sigma, 1)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)| \rightarrow 0$  である。これは、次のようにして分かる。

$\sigma \rightarrow 1$  のとき  $L(\sigma + it, \chi)^4 = O((\sigma - 1)^4)$  なのに対して、 $L(\sigma, 1) = O((\sigma - 1)^3)$ ,  $L(\sigma + 2it, \chi^2) = O(1)$  である。ここで、素直にうなずいてはいけません。 $\chi^2$  が単位指標で、かつ  $L(1, \chi) = 0$  の場合 (つまり  $t = 0$  の場合) を考えると、あら悲劇、 $L(\sigma + 2it, \chi^2) = O(1/(\sigma - 1))$  となって、 $|L(\sigma, 1)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)| \rightarrow 0$  とはいえません。ですから  $L(1, \chi) \neq 0$  をいっておかないといけません。<sup>6</sup>

**補題 4.6.**  $\chi$  が単位指標でないとき  $L(1, \chi) \neq 0$  である。

この補題は証明しませんが、この補題及びここから「Dirichlet の算術級数定理」が従うことを去年の部誌には書いてあるので証明を知りたい方はそち

---

<sup>6</sup>正確には、 $\chi^2$  が単位指標となる指標  $\chi$  についてのみこれを示せば十分です。このような  $\chi$  を実指標と呼びます。これに対して他の指標は複素指標と呼ばれます。この実指標・複素指標の区別は実は算術級数中の素数分布を扱う上で結構本質的な困難として現れてくる (らしい) のです。ここでの場合と同様、複素指標のほうが扱いやすいらしいです。

らを参照してください。また [3, 4, 5] にも証明は (それぞれ違う方針で) 載っています。

従ってこれは矛盾であると分かり、 $L(s, \chi)$  が  $\operatorname{Re}(s) \geq 1$  で零点を持たないと証明できました。

$L(s, \chi)$  の Euler 積表示において両辺の対数をとって微分して、

$$-\frac{L'}{L}(s, \chi) = \sum_p \frac{\chi(p) \log p}{p^s - \chi(p)} = \sum_p \frac{\chi(p) \log p}{p^s} + \frac{\chi(p)^2 \log p}{p^s(p^s - \chi(p))}$$

ここで、一番最後の式の第二項は  $\operatorname{Re}(s) > 1/2$  で (絶対) 収束することから、 $\sum_p \frac{\chi(p) \log p}{p^s}$  は  $L(s, \chi)$  の零点と極を除く点で正則であるとわかる。

$\Phi_{m,a}(s) = \sum_{p, \chi} \chi(a)^{-1} \chi(p) \frac{\log p}{p^s}$  で、今この和の中で  $\Phi_{m,a}(s)$  の極を作り出す

のに寄与するのは  $s = 1$  における  $\frac{L'}{L}(s, 1)$  の極のみであり、それは

$$\frac{L'}{L}(s, 1) = \frac{\zeta'}{\zeta}(s) + \sum_{p|m} \frac{1 + p^{-s} \log p}{1 - p^{-s}}$$

でありこの右辺第二項は  $s = 1$  で正則であるため、結局  $\Phi(s)$  と同じ留数であることが分かります。

□

**命題 4.7.**  $\int_1^\infty \frac{\theta_{m,a}(x) - x}{x^2} dx$  は収束する。

**証明.**

$$\begin{aligned} \Phi_{m,a}(s) &= \sum_{p, \chi} \chi(a)^{-1} \chi(p) \frac{\log p}{p^s} = \phi(m) \sum_{p \equiv a \pmod{m}} \frac{\log p}{p^s} \\ &= \int_1^\infty \frac{d\theta_{m,a}(x)}{x^s} = s \int_1^\infty \frac{\theta_{m,a}(x)}{x^{s+1}} dx \\ &= s \int_0^\infty e^{-st} \theta_{m,a}(e^t) dt \end{aligned}$$

となって、あとは命題 3.6 の証明とまったく同じです。ここで指標の直交関係を使いました。

というより、天下り的に見えた  $\Phi_{m,a}(s)$  の設定は、実は  $\operatorname{mod} m$  で  $a$  に合同な素数のみを取り出すことと、 $L(s, \chi)$  と何らかの関連を持たせることを両立させた結果なのです。つまりこの命題が証明できるように  $\Phi_{m,a}$  をとったわけです。

□

**命題 4.8.**  $\theta_{m,a}(x) \sim x$

ここからの流れは全て素数定理の証明のときとまったく同じなので、省略します。

## 5 $\mathbb{Z}[i]$ での素数定理との関係

(このセクションでは去年の僕の記事などで  $\mathbb{Z}[i]$  についてある程度知っていることを仮定します。)

ノルムが  $x$  以下の素イデアルの個数を  $\pi_{\mathbb{Z}[i]}(x)$  と書くことにします。今  $\mathbb{Z}[i]$  での素イデアルにどのようなものがあるかちよつと振り返って落ち着いて考えればすぐに、

$$\pi_{\mathbb{Z}[i]}(x) = 2\pi_{4,1}(x) + \pi_{4,3}(\sqrt{x}) + 1 \sim \frac{x}{\log x}$$

が従います。

さらにさらに、実は素イデアル定理自体は任意の代数体上で成り立ちます。しかしこれを証明することはとても僕の力量が及ぶところではないので証明は割愛します。

## 6 あとがき

ふうううう、やっと書き終わりました。締切ギリギリ。今年はギリギリまで解けなくて（というかこの方針があることをすっかり忘れていて）あせりました。

この「算術級数の素数定理」は、 $\text{mod } m$  で素数が均等に存在することを表しています。ここで、去年も似たようなことを書いたのですが、去年のネタ「算術級数定理」で示されるのは、

$$\frac{\sum_{p \in A} \frac{1}{p^s}}{\log \frac{1}{s-1}} \sim k \in \mathbb{R} \quad (s \rightarrow 1)$$

なる  $k$  を  $A$  の密度というときに、 $\text{mod } m$  の全ての既約剰余類の密度が等しいことをいうものでした。これに対して、

$$\frac{x \text{ 以下の } A \text{ に属する素数の個数}}{\pi(x)} \rightarrow k \quad (x \rightarrow \infty)$$

の時に  $A$  の自然密度は  $k$  であるというのですが、その自然密度も全ての既約剰余類について等しいことが示されたのでした。後者のほうが確かに「自然」に「個数が等しい」みたいなイメージをもてますね。

この素数定理の証明法は比較的初学者にもわかりやすいものですが、残念ながらこれ以上の理論的発展の余地はあまりないでしょう。すくなくとも一般的ではないです。オーソドックスな？やり方は、リーマンの明示式と呼ばれる次の式（もしくは、いくつもあります、それに同値な式）を示します。

$$\sum_{m=1}^{\infty} \frac{1}{m} \pi(x^{1/m}) = \text{Li}(x) - \sum_{\rho} \text{Li}(x^{\rho}) + \int_x^{\infty} \frac{dt}{t(t^2-1)\log t} - \log 2$$

ここで  $\text{Li}(x) = \int_2^{\infty} \frac{dt}{\log t} \sim \frac{x}{\log x}$  です。また  $\rho$  は  $\zeta(s)$  の非自明零点のことです。ここから  $\zeta(s)$  の零点が  $\text{Re}(s) < 1$  にしかないことを示し、適当に積分を評価したりすると素数定理が従います。 $\pi_{m,a}(x)$  についても  $L(s, \chi)$  について同様に考えます。このやり方に従うことで、 $\zeta(s)$  の零点の研究と素数分布の研究が結びつきます。たとえば  $\pi(x)$  と  $\text{Li}(x)$  がどれくらいずれているのか（誤差項の評価）なども重要ですし、一番有名な例ではリーマン予想は「 $\zeta(s)$  の非自明な零点は全て  $\text{Re}(s) = 1/2$  を満たす」でした。この予想が素数分布にとって重要なわけもこうしてリーマンの明示式をみるとほんの少し分かります。

この部誌を読んだ感想、間違いの指摘などは [s.genki0605@gmail.com](mailto:s.genki0605@gmail.com) までどうぞ。

また、数学研究部の HP (<http://f59.aaa.livedoor.jp/~nadamath/>) では、過去の部誌、入試模試などを見ることができます。ぜひ一度訪問してみてください。（やたら今年の記事で引用した去年の記事もおいてあります。）

今年で部誌を書くのも最後です。さして優れた記事を書いて来たわけではないですが 5 年間続いた 4 月はじめの苦しい習慣とお別れと思うと感慨深いです。今までお付き合いいただいた全ての方々に感謝の意を込めて、筆をおきたいと思います。

## 参考文献

- [1] D.Zagier *Newman's Short Proof of the Prime Number Theorem (the American Mathematical Monthly, Vol.104, No.8, 705-708)*
- [2] G.H.Hardy, E.M.Wright 「数論入門 I, II」 (シュプリンガー数学クラシックス, 2001)
- [3] T.M.Apostol *Introduction to Analytic Number Theory* (Springer, 1976)
- [4] Jean-Pierre Serre *A Course in Arithmetic* (Springer, 1973)

- [5] 加藤和也, 黒川信重, 斉藤毅 「数論 I -Fermat の夢と類体論」 (岩波書店,2005)
- [6] 高木貞治 「解析概論」 (岩波書店、1983)
- [7] 笠原皓司 「微分積分学」 (サイエンス社、1974)
- [8] R.v.Churchill,J.W.Brown 「複素関数入門」 (数学書房,1989)