解析的整数論に関するノート

大佐

2019 年 9 月 17 日

このノートについて

このノートは，Ram Murty 教授の，The Institute of Mathematical Sciences, Chennai(IMSc) における解析的整数論の講義をまとめたノートである[1]．本稿は，あくまで講義のまとめと，それの補足に終始しているため，一般的な数学書の体裁を取っていない．しかし，順に読み進めていけば，理解していけるように書いたつもりである．

第 I 部
素数分布論

1　解析的整数論について

解析的整数論とは，その名の通り解析的な道具を用いて数論的な問題を研究する分野である．解析といっても色々ある．例えば，実解析，複素解析，p 進解析などは一例である．p 進数は現代の数論において重要な分野の一つである

[1] 講義動画は
https://www.youtube.com/watch?v=6J-47Qk4ffY&list=PLhkiT_RYTEU1H7OmRVF5VJi76D2Efwf7F にアップロードされている．(2019/9/8 現在)

が，今回の講義（そして当然ながらこのノートも）では実解析と複素解析に話を絞る．

解析的整数論の研究対象は主に数論的関数である．例えば，数論的関数 $f(n)$ の増加の仕方であったり，それの部分和 $\sum_{n\leq x} f(n)$ の振る舞いを研究していくのが，一般的によく行われている．

2 数論的関数

数論的関数はいくつかの種類に分類できる．

2.1 乗法的関数

$$(m,n)=1 \Rightarrow f(mn)=f(m)f(n)$$

となる関数 f を乗法的関数という．また，m,n の関係性にかかわらず，$f(mn)=f(m)f(n)$ となる関数を完全乗法的関数という．例えば，約数の個数の数を返す約数関数 $d(n)$ などは乗法的関数である．まず，$d(n)$ に具体的な n の値を入れたときの値を見てみる．

$$d(2)=d(3)=d(5)=2$$

$$d(6)=4$$

ここで実際,

$$d(6)=d(2\cdot 3)=d(2)d(3)$$

となっていることがわかる．これを証明してみよう．

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$$

とおき，δ が n を割り切るとする．すると

$$\delta = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

と表せる．当然のことながら，$0 \leq \beta_i \leq \alpha_i$ である．そして，このような $\beta_1, \beta_2 \dots \beta_k$ の選び方と，$d(n)$ の値は一致するから，

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

と表せる．ここから，これが乗法的関数であることがわかる．しかし，これは完全乗法的関数ではない．

$$4 = d(8) \neq d(2)^3 = 8$$

は反例の一つである．また，オイラーの φ 関数も乗法的な関数の一例である．$\varphi(n)$ は，n 以下の，n と互いに素な自然数の数を返す関数である，これを証明してみよう．

まず，$(a, b) = 1$ とする．そして，x, y を $1 \leq y \leq a, 0 \leq x \leq b - 1$ を満たす整数とする．ここで，$t = ax + y$ とおく．すると，t は 1 以上 ab 以下の自然数全てをわたる．さて，ここで，$(a, y) = 1$ ならば，$(t, a) = 1$ となる．逆も明らかに成り立つ．このような y は $\varphi(a)$ 個ある．そして，y を固定した時，$ax + y$ で表される数は b 個あるが，それらを b で割った余りは全て異なる．なぜなら，もし $ax_1 + y \equiv ax_2 + y \pmod{b}$ とすると，$a(x_1 - x_2) \equiv 0 \pmod{b}$ となって，これは $(a, b) = 1$ という仮定に反するからだ．したがって，これら b 個の中に $(t, b) = 1$ なるものは $\varphi(b)$ 個ある．したがって，$(a, t) = (b, t) = 1$ なる t は $\varphi(a)\varphi(b)$ 個ある．よって，$\varphi(ab) = \varphi(a)\varphi(b)$ となって，$\varphi(n)$ は乗法的関数である． しかし，これもまた完全乗法的関数ではない．

$$\varphi(p^j) = p^{j-1}(p - 1) \neq \varphi(p)^j = (p - 1)^j$$

は簡単な反例の一つである．また，オイラーの φ 関数の面白い性質の一つとして，

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つということが挙げられる．これを証明してみよう[2]．

さて，まず，n と互いに素な n 以下の自然数を，$x_1, x_2, \ldots x_{\varphi(n)}$ とおく．ここで，

$$x_i \equiv x_j \pmod{n} \Rightarrow i = j$$

となることは明らかであろう．さて，これのそれぞれに a をかけた，

$$ax_1, ax_2, \ldots ax_{\varphi(n)}$$

を考察してみよう．実は，これを n で割った余りは $x_1, x_2, \ldots x_{\varphi(n)}$ と 1 対 1 に対応しているのだ．まず，

$$ax_i \equiv ax_j \pmod{n} \Rightarrow i = j$$

を示そう．もし，$ax_i \equiv ax_j \pmod{n}$ ならば，$n|(ax_i - ax_j) = a(x_i - x_j)$ である，すると，$(a, n) = 1$ より $n|(x_i - x_j)$ であるが，$-n < x_i - x_j < n$ だから，$x_i - x_j = 0 \Leftrightarrow x_i = x_j \Leftrightarrow i = j$.

次に，ax_i を n で割ったあまりが $x_1, x_2, \ldots x_{\varphi(n)}$ の中にあることを示そう．もしなかったと仮定すると，

$$ax_i \equiv k \pmod{n}, (n, k) \neq 1$$

なる k が存在する．すると，$ax_i = bn + k$ とかけるが，左辺が n と互いに素なのに対して，右辺が n と共通因数を持ってしまうから矛盾である．したがって，$ax_1, ax_2, \ldots ax_{\varphi(n)}$ を n で割った余りは $x_1, x_2, \ldots x_{\varphi(n)}$ と 1 対 1 対応する．

ここで，$x_1, x_2, \ldots x_{\varphi(n)}$ と $ax_1, ax_2, \ldots ax_{\varphi(n)}$ それぞれ掛け合わせると，

$$a^{\varphi(x)}(x_1 x_2 \ldots x_{\varphi(n)}) \equiv x_1 x_2 \ldots x_{\varphi(n)} \pmod{n}$$

となる．$(x_1 x_2 \ldots x_{\varphi(n)}, n) = 1$ より，

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

[2]ここでの証明は高木貞治「初等整数論講義」を参考にした.

となる.

2.2 加法的関数

$$(m,n)=1 \Rightarrow f(mn)=f(m)+f(n)$$

となる関数 f を加法的関数という．また，m,n の関係性にかかわらず $f(mn)=f(m)+f(n)$ となる場合は，完全加法的関数という．例えば，n を割り切る素数 p の数を返す関数 $\omega(n)$ は，加法的関数である．これは明らかであろう．しかしながら，これは完全加法的関数ではない．例えば,

$$\omega(p^2)=1 \neq \omega(p)+\omega(p)=2$$

が反例である．今度は完全加法的関数の例を挙げる．$n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ に対して，$\Omega(n)=\alpha_1+\alpha_2+\cdots+\alpha_k$ と定義すれば，これが完全加法的関数であることは明らかであろう．

2.3 その他の関数

フォン・マンゴルトの関数と呼ばれる関数がある．

$$\Lambda(n)=\begin{cases}\log p & n=p^a, p\ is\ prime\\ 0 & otherwise\end{cases}$$

と定義される関数で，これは加法的関数でも，乗法的関数でもない．しかし，これは大変重要な数論的関数である．この関数が持つ面白い性質として,

$$\log n=\sum_{d|n}\Lambda(d)$$

ということが挙げられる．これは，例によって $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ と置いたとき,

$$\log n=\alpha_1\log p_1+\alpha_2\log p_2+\cdots+\alpha_k\log p_k$$

とかけることと，n 以下の自然数に，p_i のべきであるような数は α_i 回現れることから直ちに導かれる．

3　アーベルの総和法

$\{a_n\}_{n=1}^{\infty}$ を複素数の数列，$f(t)$ を $t \geq 0$ で微分可能な関数として，$A(x) = \sum_{n \leq x} a_n$ とおくと，

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt$$

となる．これをアーベルの総和公式といい，解析的整数論における非常に有用な道具である．離散的な和を，積分に変換できることの意味は大きい．では，これを証明していこう．

まず，$a_n = A(n) - A(n-1)$ であることに注意しよう．すると，

$$\begin{aligned}
\sum_{n \leq x} a_n f(n) &= \sum_{n \leq x} (A(n) - A(n-1))f(n) \\
&= \sum_{n \leq x} A(n)f(n) - \sum_{n \leq x} A(n-1)f(n) \\
&= \sum_{n \leq x} A(n)f(n) - \sum_{n \leq x-1} A(n)f(n+1) \\
&= A(x)f(x) + \sum_{n \leq x-1} A(n)(f(n) - f(n+1)) \\
&= A(x)f(x) + \sum_{n \leq x-1} \left(- \int_n^{n+1} A(t)f'(t)dt \right) \\
&= A(x)f(x) - \int_1^x A(t)f'(t)dt
\end{aligned}$$

となる．したがって，標記の等式は示された．

では，この公式を実際に使ってみよう．

$$\sum_{n \leq x} \frac{1}{n}$$

について考えてみる．$a_n = 1, f(t) = 1/t$ とおくと，$A(t) = \lfloor t \rfloor$ である．これをアーベルの総和公式に代入してみる．すると，

$$\sum_{n \leq x} \frac{1}{n} = \lfloor x \rfloor \frac{1}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2} dt \tag{1}$$

となる．ここで，ランダウのビッグオー記法を導入しよう．ちなみに，余談であるが，このランダウは，ランダウ＝リフシッツの理論物理学教程の著者のランダウとは別人である．さて，$x \to \infty$ で

$$f(x) = O(g(x))$$

というのは，ある定数 k が存在して，

$$|f(x)| \leq k|g(x)|$$

が十分大きな x について成り立つことである．本稿では，単に $O(g(x))$ といった時，特に断らない限り，常に $x \to \infty$ の時の挙動を意味することにする．例えば，$x^2+5x+1 = O(x^2)$ となる．ここで，この記法を用いると，$\lfloor x \rfloor = x+O(1)$ であるから，(1) は，

$$\sum_{n \leq x} \frac{1}{n} = \frac{x + O(1)}{x} + \int_1^x \frac{t + O(1)}{t^2} dt = 1 + O\left(\frac{1}{x}\right) + \log x + \int_1^x \frac{O(1)}{t^2} dt$$

と書けて，また $\int_1^\infty \frac{O(1)}{t^2} dt$ は収束するから，結局，

$$\sum_{n \leq x} \frac{1}{n} = \log x + O(1)$$

となる．また，これをもっと精密に近似することも可能である．$\{x\}$ を x の小数部分とする．すると，$\lfloor x \rfloor = x - \{x\}$ である．ここで，これを用いて (1) を書き直すと，

$$\sum_{n \leq x} \frac{1}{n} = \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{x\}}{t^2} dt = 1 + O\left(\frac{1}{x}\right) + \log x - \int_1^x \frac{\{x\}}{t^2} dt$$

となる．そして，$C = \int_1^\infty \frac{\{x\}}{t^2} dt$ とおくと，

$$\int_1^x \frac{\{x\}}{t^2} dt = \int_1^\infty \frac{\{x\}}{t^2} dt - \int_x^\infty \frac{\{x\}}{t^2} = C + O\left(\frac{1}{x}\right)$$

となり，結局，

$$\sum_{n \leq x} \frac{1}{n} = 1 - C + \log x + O\left(\frac{1}{x}\right)$$

となる，そして，$1 - C$ はオイラーの定数 γ に等しい．

もう一つアーベルの総和法の例をあげよう．

$$\sum_{n \leq x} \log n$$

について考えてみる．例のように，$a_n = 1, f(t) = \log t, A(t) = \lfloor t \rfloor$ として，

$$\sum_{n \leq x} \log n = \lfloor x \rfloor \log x - \int_1^x \frac{\lfloor t \rfloor}{t} dt$$

ここで，$\lfloor x \rfloor = x + O(1)$ であったことに注意すると，

$$\begin{aligned}
\sum_{n \leq x} \log n &= \lfloor x \rfloor \log x - \int_1^x \frac{\lfloor t \rfloor}{t} dt \\
&= (x + O(1)) \log x - \int_1^x \frac{t + O(1)}{t} dt \\
&= x \log x + O(\log x) - (x - 1) + O(\log x) \\
&= x \log x - x + O(\log x)
\end{aligned}$$

が導ける．これも (1) と同じように精密に近似することができるだろうが，これは本節の目的を超えるであろう．

4　素数計数関数に関するチェビシェフの不等式

節の名前が長いので，単にチェビシェフの不等式と書きたいのであるが，単にそう書くと確率論の定理になってしまう．ただし，本稿においては，チェビ

シェフの不等式とは，素数計数関数に関するチェビシェフの不等式を指すこととする．さて,「素数計数関数に関する」不等式，であるから，これは素数計数関数

$$\pi(x) = number\ of\ primes \leq x$$

に対する結果である．ガウスが 10 代の頃,，$\pi(x) \sim x/\log x$ と予想したことは有名である．これは，アダマールとプーサンによって 18 世紀後半に証明され，素数定理と呼ばれるようになった．素数定理を示すのは，本稿の大きな目標の一つである．そして，その 50 年ほど前，チェビシェフがこれに近い形で $\pi(x)$ を評価できることを証明した．定理の主張を書いた方がわかりやすいであろう．

定理 1. ある定数，$A, B > 0$ が存在して，$x \geq 2$ に対して

$$\frac{Ax}{\log x} \leq \pi(x) \leq \frac{Bx}{\log x}$$

となる．

これは，アーベルの総和法を用いて示せる，大きな結果である．では，証明していこう．

4.1 メルテンスの第一定理

フォン・マンゴルトの関数を使うと，

$$\log n = \sum_{d|n} \Lambda(d)$$

であったことを思い出そう．また，

$$\sum_{n \leq x} \log x = x \log x - x + O(\log x)$$

であった．そして，

$$\sum_{n \leq x} \log x = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{d \leq x} \Lambda(d) \sum_{n \leq x, d|n} 1$$

が成り立つ．これは，$\Lambda(d)$ が何回現れるかに注意すれば導ける．つまり，$\Lambda(d)$ は x 以下の d の倍数の個数，つまり $\sum_{n\leq x, d|n} 1$ 回現れるのである．そして，$\sum_{n\leq x, d|n} 1 = \lfloor \frac{x}{d} \rfloor$ であることに注意すると，

$$\sum_{n\leq x}\sum_{d|n}\Lambda(d) = \sum_{d\leq x}\Lambda(d)\left\lfloor\frac{x}{d}\right\rfloor = \sum_{d\leq x}\Lambda(d)\left(\frac{x}{d}+O(1)\right)$$

となる．さて，ここで，

$$\psi(x) = \sum_{d\leq x}\Lambda(d)$$

と定義する．これを，第二チェビシェフ関数という．そして，

$$\psi(x) = O(x)$$

と仮定すると，

$$\begin{aligned}&\sum_{d\leq x}\Lambda(d)\left(\frac{x}{d}+O(1)\right) = x\sum_{d\leq x}\frac{\Lambda(d)}{d} + O(x) = x\log x - x + O(\log x)\\ \Rightarrow &\sum_{d\leq x}\frac{\Lambda(d)}{d} = \log x + O(1) \qquad (2)\end{aligned}$$

となる．これは，メルテンスの第一定理といい，大きな成果であるが，$\psi(x) = O(x)$ を仮定して得られた結果である．したがって，これを使うためには $\psi(x) = O(x)$ を示す必要がある．

4.2 チェビシェフ関数と素数定理の関係

前節で第二チェビシェフ関数というものが出てきたが，当然第一もある．ここで，

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

と定義する．これを第一チェビシェフ関数という．当然のことながら，$\vartheta(x) \leq \psi(x)$ である．また，$\psi(x)$ は素数のべきを，$\vartheta(x)$ に比べて余分に数えている

が，例えば p^2 となるものだけ数えた時，これは $\vartheta(x^{\frac{1}{2}})$ に等しい．つまり，

$$\psi(x) = \vartheta(x) + \vartheta(x^{\frac{1}{2}}) + \vartheta(x^{\frac{1}{3}}) \cdots = \sum_{n=1}^{\infty} \vartheta(x^{\frac{1}{n}})$$

が成り立つ．そして，

$$\sum_{n=1}^{\infty} \vartheta(x^{\frac{1}{n}}) = \sum_{n=1}^{\infty} \sum_{p \leq x^{\frac{1}{n}}} \log p = \sum_{p \leq x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor$$

だから，

$$\begin{aligned} \psi(x) - \vartheta(x) &= \sum_{p \leq x} \log p \left(\left\lfloor \frac{\log x}{\log p} \right\rfloor - 1 \right) \\ &= \sum_{p \leq x^{\frac{1}{2}}} \log p \left(\left\lfloor \frac{\log x}{\log p} \right\rfloor - 1 \right) \\ &\leq \sum_{p \leq x^{\frac{1}{2}}} \log x \leq x^{\frac{1}{2}} \log x \end{aligned}$$

となって，

$$\psi(x) = \vartheta(x) + O(x^{\frac{1}{2}} \log x)$$

である．さて，ここで，

$$\vartheta(x) \sim x \Leftrightarrow \psi(x) \sim x \Leftrightarrow \pi(x) \sim \frac{x}{\log x}$$

を示そう[3]．$\psi(x) = \vartheta(x) + O(x^{\frac{1}{2}} \log x)$ より，$\vartheta(x) \sim x$ または $\psi(x) \sim x$ を仮定すると，$\psi(x) \sim \vartheta(x)$ だから，$\vartheta(x) \sim x \Leftrightarrow \psi(x) \sim x$ は問題ないだろう．よって，

$$\vartheta(x) \sim x \Leftrightarrow \pi(x) \sim \frac{x}{\log x} \tag{3}$$

[3] この証明は，二本松せきゅーん氏の `https://note.mu/integers_blog/n/nd43c35709f93` の証明を大いに参考にした．(最終閲覧日：2019 年 8 月 13 日)

を示せば十分である．ここで，

$$f(x) = \frac{1}{\log x}, a_n = \begin{cases} \log n & n\,is\,prime \\ 0 & otherwise \end{cases}$$

とおくと，

$$\sum_{2 \leq n \leq x} a_n f(n) = \pi(x)$$

となる．非常に賢いアイデアだと感じる．さて，これにアーベルの総和法を適用しよう．$\sum_{n \leq x} a_n = \vartheta(x)$ に注意すると，

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt$$

となる．ここで，両辺を $\frac{x}{\log x}$ で割る．

$$\frac{\pi(x)}{\frac{x}{\log x}} = \frac{\vartheta(x)}{x} + \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt$$

よって，第二項が 0 に収束することを仮定すれば，$\vartheta(x) \sim x \Rightarrow \pi(x) \sim \frac{x}{\log x}$ が示せる．では第二項が 0 に収束することを示そう．ここで，

$$\int_2^x \frac{dt}{(\log t)^2} = \int_2^{\sqrt{x}} \frac{dt}{(\log t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\log t)^2} \leq \frac{\sqrt{x}}{(\log 2)^2} + \frac{x}{(\log \sqrt{x})^2}$$

で，$\frac{x}{(\log \sqrt{x})^2} = \frac{4x}{4(\log \sqrt{x})^2} = \frac{4x}{(\log x)^2}$ だから，

$$\int_2^x \frac{dt}{(\log t)^2} = O\left(\frac{x}{(\log x)^2}\right)$$

$\vartheta(x) \sim x$ を仮定すると，$\vartheta(x) = O(x)$ なので，

$$\int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = O\left(\frac{x}{(\log x)^2}\right)$$

となり，

$$\frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = \frac{\log x}{x} \cdot O\left(\frac{x}{(\log x)^2}\right) = O\left(\frac{1}{\log x}\right) \to 0$$

であるから，$\vartheta(x) \sim x \Rightarrow \pi(x) \sim \frac{x}{\log x}$ が示された．逆も同様に示せる．

$$f(x) = \log x, a_n = \begin{cases} 1 & n\ is\ prime \\ 0 & otherwise \end{cases}$$

とおくと，

$$\sum_{2 \leq n \leq x} a_n f(n) = \vartheta(x)$$

となり，$\sum_{n \leq x} a_n = \pi(x)$ に注意して，

$$\vartheta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt \Rightarrow \frac{\vartheta(x)}{x} = \frac{\pi(x)}{\frac{x}{\log x}} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt$$

となるから，今回も $\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt \to 0$ を示せば良い．ここで，部分積分を用いて，

$$\int_2^x \frac{dt}{\log t} \leq \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) = O\left(\frac{x}{\log x}\right)$$

となるので，$\pi(x) \sim \frac{x}{\log x}$ の仮定から，

$$\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = O\left(\frac{1}{x} \int_2^x \frac{1}{\log t} dt\right) = O\left(\frac{1}{\log x}\right) \to 0$$

となり，$\vartheta(x) \sim x \Leftarrow \pi(x) \sim \frac{x}{\log x}$ が示された．よって，(3) が成立する．

4.3 チェビシェフの不等式の証明

さて，ここで，$\binom{2n}{n}$ について考察しよう．まず，これは $(1+1)^{2n}$ を二項定理を用いて展開したものの中に現れるから，明らかに，

$$\binom{2n}{n} \leq 2^{2n}$$

である．そして，$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ からわかる通り，これは $n < p \leq 2n$ なる全ての素数 p で割り切ることができる．したがって，

$$\prod_{n < p \leq 2n} p \mid \binom{2n}{n} \leq 2^{2n}$$

が言える．これらをつなげると，

$$\left(\prod_{n<p\leq 2n} p\right) \leq 2^{2n} \Rightarrow \sum_{n<p\leq 2n} \log p \leq 2n\log 2$$

となり，矢印の右側での左辺に注目すると，これが $\vartheta(2n)-\vartheta(n)$ であることがわかるから，

$$\vartheta(2n)-\vartheta(n) \leq 2n\log 2$$

である．そして，これは n の値にかかわらず成立するから，

$$\begin{aligned}
\vartheta(2n)-\vartheta(n) &\leq 2n\log 2\\
\vartheta(n)-\vartheta\left(\frac{n}{2}\right) &\leq n\log 2\\
&\vdots
\end{aligned}$$

となる．これらを全て足すと，

$$\vartheta(2n) \leq 4n\log 2$$

が導けて，これは，

$$\vartheta(x) = O(x)$$

を意味している．そして，ここから題意の不等式の右半分が導ける．つまり，

$$\pi(x) \leq \frac{Bx}{\log x}$$

となる B が存在することが示せる．まず，$\vartheta(x)=O(x)$ は，ある定数 K が存在して，十分大きい x に対して

$$\sum_{p\leq x} \log p \leq Kx$$

が成立する，という意味である．そして，

$$\sum_{\sqrt{x}<p\leq x} \log p < \sum_{p\leq\sqrt{x}} \log p + \sum_{\sqrt{x}<p\leq x} \log p = \sum_{p\leq x} \log p$$

であり，

$$(\pi(x)-\pi(\sqrt{x}))\log\sqrt{x}\le\sum_{\sqrt{x}<p\le x}\log p$$

となるから，

$$(\pi(x)-\pi(\sqrt{x}))\log\sqrt{x}=\frac{1}{2}(\pi(x)-\pi(\sqrt{x}))\log x<Kx$$

となる．また，ここで，当然 $\pi(\sqrt{x})\le\sqrt{x}$ だから，

$$\pi(x)\log x-\sqrt{x}\log x\le(\pi(x)-\pi(\sqrt{x}))\log x\le 2Kx$$

となって，

$$\pi(x)\le\frac{2Kx}{\log x}+\sqrt{x}$$

となり，$\sqrt{x}=O(x/\log x)$ だから，ある定数 B が存在して，

$$\pi(x)\le\frac{Bx}{\log x}$$

となる．次に，ある定数 $0<A$ が存在して，

$$\frac{Ax}{\log x}\le\pi(x)$$

となることを示そう．これには，(2) を用いる．つまり，

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

を用いる．これは，$\psi(x)=O(x)$ を仮定して得られた結果だったが，$\vartheta(x)=O(x)$ を示したからこれはすでに示されている．さて，これは，

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

を導く[4]．なぜなら，これら二つの右辺の違いは，素数のべきが入るか入らないかだが，素数のべきによる和，つまり $\frac{\log p}{p^k}$ の和は収束する．つまり，

$$\sum_{p}\sum_{k=2}^{\infty}\frac{\log p}{p^k}$$

[4]むしろ，普通はこちらをメルテンスの第一定理という．

は収束する．これは，例えば，

$$\sum_p \sum_{k=2}^{\infty} \frac{\log p}{p^k} = \sum_p \frac{\log p}{p^2} \frac{1}{1-\frac{1}{p}} < 2 \sum_p \frac{p^{\frac{1}{2}}}{p^2} = 2 \sum_p \frac{1}{p^{\frac{3}{2}}}$$

などとすれば示せる．さて，定数 D に対して，

$$\sum_{\frac{x}{D} < p \leq x} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} - \sum_{p \leq \frac{x}{D}} \frac{\log p}{p} = \log x - \log \frac{x}{D} + O(1) = \log D + O(1)$$

であるから，D を十分大きくとれば，ある定数 C_0 があって，

$$C_0 \leq \sum_{\frac{x}{D} \leq p \leq x} \frac{\log p}{p}$$

となる．さてここで，

$$\sum_{\frac{x}{D} \leq p \leq x} \frac{\log p}{p} \leq \left(\pi(x) - \pi\left(\frac{x}{D}\right) \right) \frac{\log x}{x/D}$$

となるから，

$$C_0 \leq \left(\pi(x) - \pi\left(\frac{x}{D}\right) \right) \frac{\log x}{x/D} \leq \pi(x) \frac{\log x}{x/D}$$

よって，

$$\frac{C_0 x/D}{\log x} \leq \pi(x)$$

となり，これは不等式の左半分を示している．したがって，ある定数，A,B が存在して，$x \geq 2$ において，

$$\frac{Ax}{\log x} \leq \pi(x) \leq \frac{Bx}{\log x}$$

となる[5]．

[5] これまでの議論は十分大きい x についてしか成り立たないのではないかと思う人もいるだろうが，$x/\log x$ は $x \geq 2$ で 0 より大きく，有界だから，十分大きい x で不等式を成り立たせる $A, B > 0$ があれば，$x \geq 2$ においてもそのような定数が存在するのである．

5　チェビシェフの定理

チェビシェフの定理は，チェビシェフの不等式よりも素数定理に幾分か近い定理である．

定理 2. もし，極限

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

が存在すれば，それは 1 以外あり得ない．

これは，どういうことかというと，$x\to\infty$ のとき極限値があれば，素数定理が成り立つということである！この大きな成果を示していこう．

まず，

$$\lim_{x\to\infty}\frac{\vartheta(x)}{x}=\alpha \tag{4}$$

となるならば，$\alpha=1$ ということを示していく．ここで，まず準備としてスモールオー記法を導入する[6]．

$$f(x)=o(g(x))$$

というのは，ある定数 k が存在して，

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$$

が成り立つことである．例えば，$\log x=o(x)$ と書ける．さて，この記法を使うと，(4) は次のように書ける．

$$\vartheta(x)=\alpha x+o(x)$$

さて，ここで，

$$\sum_{p\le x}\frac{\log p}{p}$$

[6] これも本稿ではビッグオーの時と同様に，特に断らなければ $x\to\infty$ の時の挙動を指すとする．

について考察する．これをアーベルの総和法を用いて書き直してみよう．

$$f(x)=\frac{1}{x}, a_n=\begin{cases}\log n & n\,is\,prime\\ 0 & otherwise\end{cases}$$

とおくと，

$$\sum_{p\leq x}\frac{\log p}{p}=\sum_{n\leq x}a_n f(n)=\frac{\vartheta(x)}{x}+\int_1^x\frac{\vartheta(t)}{t^2}dt$$

ここで，$\frac{\vartheta(x)}{x}=O(1)$ で，$\vartheta(x)=\alpha x+o(x)$ だったから，

$$\sum_{p\leq x}\frac{\log p}{p}=O(1)+\int_1^x\frac{\alpha t+o(t)}{t^2}dt$$

そして，第二項の積分は，$o(t)$ を無視できると考えると，$\alpha\log x$ になる．したがって，

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

であったから，$\alpha=1$ でなければならない．これを厳密に示そう．ここで，

$$\int_1^x\frac{\alpha t+o(t)}{t^2}$$

について考察していく．まず，積分範囲を適当な y によって分割する．

$$\int_1^x\frac{\alpha t+o(t)}{t^2}=\int_1^y\frac{\alpha t+o(t)}{t^2}+\int_y^x\frac{\alpha t+o(t)}{t^2}$$

ここで，y を x の関数，$y=e^{\sqrt{\log x}}$ とする．さて，次に第二項の積分について考察しよう．スモールオーの定義から，任意の $\varepsilon>0$ に対して，ある y が対応して $y<t\Rightarrow|\vartheta(t)-\alpha t|<\varepsilon t$ である．(当然それに対応して x も決まる.) すると，

$$\int_y^x\frac{\alpha t+o(t)}{t^2}<\alpha\log\frac{x}{y}+\int_y^x\frac{\varepsilon}{t}=(\alpha+\varepsilon)\log\frac{x}{y}=(\alpha+\varepsilon)(\log x-\sqrt{\log x})$$

だから，

$$\int_y^x\frac{\alpha t+o(t)}{t^2}=(\alpha+\varepsilon)\log x+O(\sqrt{\log x})$$

である．そして，第一項の積分は，$\vartheta(x) = O(x)$ だったから，

$$\int_1^y \frac{O(t)}{t^2} = O(\log y) = O(\sqrt{\log x})$$

よって，

$$\int_1^x \frac{\alpha t + o(t)}{t^2} = (\alpha + \varepsilon)\log x + O(\sqrt{\log x})$$

である．ここで $\alpha \neq 1$ とすると，ε は任意であり，十分大きい x に対して，$\log x = O(\sqrt{\log x})$ となってしまうから，$\alpha = 1$ でなければならない．さて，ここで，(4.2) の議論を思い出そう．すると，もし

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

ならば，

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = \alpha$$

だとわかる．したがって，今示したことから，$\alpha = 1$ でなくてはならない．つまり，チェビシェフの定理は示されたのである．

6　解析的整数論における級数

6.1　アーベルの連続性定理

今，冪級数

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

が $|x| < 1$ の範囲で絶対収束するとする．そして，

$$\sum_{n=0}^{\infty} a_n$$

が収束するとする．すると，

$$\lim_{x\to 1-0} \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n$$

となる．これはアーベルの連続性定理と呼ばれる．今，これを示しておこう[7]．

まず，$\sum a_n$ が収束するから，任意の $\delta > 0$ に対して，十分大きな n をとって，

$$\sigma_m = \sum_{k=n}^{n+m} a_k, |\sigma_m| < \delta$$

となるようにできる．そこで，$0 \leq x \leq 1$ とすれば，

$$\left| \sum_{k=n}^{n+m} a_k x^k \right|$$
$$= |\sigma_0(x^n - x^{n+1}) + \sigma_1(x^{n+1} - x^{n+2}) + \cdots + \sigma_{m-1}(x^{n+m-1} - x^{n+m}) + \sigma_m x^{n+m}|$$
$$\leq \delta x^n \leq \delta$$

となり，δ は任意であったから，これは $0 \leq x \leq 1$ で一様収束する．つまり，

これは $0 \leq x \leq 1$ で連続だから，

$$\lim_{x \to 1-0} \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n$$

となる．例をあげて説明しよう．

$$-\log(1+x) = \sum_{n=1}^{\infty} (-1)^n \frac{x^n}{n}$$

が，$|x| < 1$ で成り立つ．また，級数 $\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$ は収束するから，

$$-\log 2 = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}$$

である．

6.2 ディリクレ級数

数列 $\{a_n\}_{n=1}^{\infty}$ に対して，s に関する関数

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

[7] この証明は，高木貞治「定本 解析概論」p.198 によった．

をディリクレ級数という．ここで，気づかれた方もおられると思うが，$a_n = 1$ とすればこれはリーマンのゼータ関数である．つまり，リーマンのゼータ関数は，ディリクレ級数の一種である．ここで，部分和

$$\sum_{n \leq x} a_n$$

を研究する際に，$\{a_n\}$ から作られるディリクレ級数を研究する，という手法が使える．例として，リーマンのゼータ関数をあげよう．

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

は，$\Re(s) > 1$ で収束する．さて，これのオイラー積表示，というと，知っている方も多いのではないだろうか．これは，

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

となることである．これは，素因数分解の一意性から導かれる．ちなみにこれは，素数の無限性の新しい証明を与える．素数が有限個しかないと仮定すると，$s \to 1$ の極限を考えれば，左辺は発散するのに対して，右辺は収束するから矛盾が生じる．

さて，1859 年，リーマンはゼータ関数の定義を，解析接続を用いて複素数全体に拡張した．ここで，$f(s), g(s)$ がそれぞれ領域 A, B で解析的，$A \subset B$ とすると，もし，$f(s) = g(s)$ が $s \in A$ なる全ての s について成り立つならば，g を f の解析接続，あるいは解析的延長という．さて，リーマンのゼータ関数を解析接続する方法について解説しよう．解析接続前のリーマンのゼータ関数部分和にアーベルの総和法を適応する．まず，$\Re(s) > 1$ なる領域を σ とおく．そして $a_n = 1, f(n) = 1/n^s$ とおくと，

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor t \rfloor}{t^{s+1}} dt$$

そして，$x \to \infty$ を考えると，

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = s \int_1^{\infty} \frac{\lfloor t \rfloor}{t^{s+1}} dt$$

である．そして，$\lfloor x \rfloor = x - \{x\}$ である（ただし $\{x\}$ は x の小数部分）．よって，

$$\zeta(s) = s \int_1^{\infty} \frac{\lfloor t \rfloor}{t^{s+1}} dt = s \int_1^{\infty} \frac{1}{t^s} dt - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt$$

ここで，第一項の積分は，s が σ 内にあるとき，

$$s \int_1^{\infty} \frac{1}{t^s} dt = \frac{s}{s-1}$$

となるから，

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt$$

さてこれの右辺は，$s = 1$ を除いて $\Re(s) > 0$ なる s で解析的である．なぜならば，$s/(s-1)$ の解析性は明らかだし，

$$\int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt$$

に関しても，任意の $\delta > 0$ に対して，$\Re(s) > \delta$ とすると，

$$\left| \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt \right| < \int_1^{\infty} \frac{\{t\}}{t^{\delta+1}} dt < \infty$$

となるから，任意の ε に対して，$\Re(s) > \delta$ なる領域で s に関係しない定数 R が存在して，$r > R$ ならば，

$$\left| \int_r^{\infty} \frac{\{t\}}{t^{s+1}} dt \right| < \varepsilon$$

とできる．したがって，$\Re(s) > \delta$ なる領域に関してこの積分は一様収束である．δ は任意であったから，結局これは，$\Re(s) > 0$ なる領域に関して一様収束するから，解析的である[8]．

[8]詳しくは，解析概論の定理 42,57 などを見よ．

この手法は一般化することが可能であろう．すなわち，

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

が $\Re(s) > 1$ で絶対収束するとして，$A(x) = \sum_{n \leq x} a_n$ とおけば，アーベルの総和法により，

$$\sum_{n \leq x} \frac{a_n}{n^s} = \frac{A(x)}{x^s} + s \int_1^x \frac{A(t)}{t^{s+1}} dt$$

である．そして，ある定数 $\theta < 1$ があって，

$$A(x) = \alpha x + O(x^\theta)$$

となるとしよう．その時．$x \to \infty$ の極限を考えると，第一項は消えて，$O(x^\theta)$ の項を $A(x) - \alpha x$ とかけば，

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \frac{\alpha s}{s-1} - s \int_1^{\infty} \frac{A(t) - \alpha t}{t^{s+1}} dt$$

そして，もし $\Re(s+1-\theta) > 1$ ならば，つまり $\Re(s) > \theta$ ならば，第二項の積分は一様収束するから，解析的である．つまり，解析接続によって，$\Re(s) > 1$ から $\Re(s) > \theta$ に定義域を広げられた．

6.3 リーマンゼータ関数と素数分布

さて，オイラー積表示からも明らかなように，

$$\Re(s) > 1 \Rightarrow \zeta(s) \neq 0$$

である．したがって，この領域で，$\log \zeta(s)$ は well-defined で，解析的である．よって

$$\log \zeta(s) = -\sum_p \log \left(1 - \frac{1}{p^s}\right)$$

ここで，冪級数展開 $\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} + \dots$ を思い出すと，

$$-\sum_{p} \log\left(1 - \frac{1}{p^s}\right) = \sum_{p\ prime, n\geq 1} \frac{1}{np^{ns}}$$

そして，この級数は項別微分ができる[9]から，

$$(\log\zeta(s))' = \frac{\zeta'(s)}{\zeta(s)} = -\sum_{p\ prime, n\geq 1} \frac{\log p}{p^{ns}} \Rightarrow -\frac{\zeta'(s)}{\zeta(s)} = \sum_{p\ prime, n\geq 1} \frac{\log p}{p^{ns}}$$

さて，ここで，右辺の級数は，次のように書き直すことができる．

$$\sum_{p\ prime, n\geq 1} \frac{\log p}{p^{ns}} = \sum_{m=1}^{\infty} \frac{\Lambda(m)}{m^s}$$

結局，まとめると，

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \tag{5}$$

が，$\Re(s) > 1$ で成り立つ．

さて，もし $\theta < 1$ があって，

$$\psi(x) = x + O(x^\theta)$$

となるとしよう．すると，$\theta < 1$ ならば，$\psi(x) \sim x$ となって，これは素数定理と同値である．そして，(5) はアーベルの総和法を用いて，次のように書き直すこともできる．

$$\begin{aligned} -\frac{\zeta'(s)}{\zeta(s)} &= s\int_1^{\infty} \frac{\psi(x)}{x^{s+1}} dx \\ &= \frac{s}{s-1} - s\int_1^{\infty} \frac{\psi(t)-t}{t^{s+1}} dt \end{aligned}$$

ここで，第二項の積分は $\Re(s) > \theta$ で解析的である．これは，当然左辺がその領域において $s = 1$ 以外で正則であることを示している．すると，$\zeta(s)$ が，その領域で零点を持たないことが導かれる．かくして，リーマンのゼータ関数が素数の分布と結びつくのである！

[9]項別に微分した結果が一様収束だから．詳しくは解析概論定理 40 をみよ．

7　ウィーナー＝池原の定理

本節ではウィーナー・池原の定理について解説する．これはタウバー型定理と呼ばれる定理である．ちなみに，ウィーナーと池原は，初期のサイバネティクス研究においての功績がよく知られている．これを学習するモチベーションの一つは，D.J.Newman による，素数定理の証明であろう．さて，まず補題を示そう．

補題 1.

$$a_n \geq 0, A(x) = \sum_{n \leq x} a_n$$

とおく．すると，

$$\int_1^{\infty} \frac{A(x) - x}{x^2} dx < \infty$$

ならば，$x \to \infty$ の際，

$$A(x) \sim x$$

である．

では，これを証明していこう．

まず，

$$A(x_i) \geq \lambda x_i$$

となる x_i が無限に存在するように，$\lambda > 1$ を定められたとしよう．続いてそのような x_i を適当にとって

$$\int_{x_i}^{\lambda x_i} \frac{A(t) - t}{t^2} dt$$

について考えよう．すると，$a_n \geq 0$ より，

$$\int_{x_i}^{\lambda x_i} \frac{A(t) - t}{t^2} dt \geq \int_{x_i}^{\lambda x_i} \frac{A(x_i) - t}{t^2} dt \geq \int_{x_i}^{\lambda x_i} \frac{\lambda x_i - t}{t^2} dt$$

となる．ここで，$t = ux_i$ と置換すると，

$$\int_{x_i}^{\lambda x_i} \frac{\lambda x_i - t}{t^2} dt = \int_1^{\lambda} \frac{\lambda x_i - ux_i}{(ux_i)^2} x_i du = \int_1^{\lambda} \frac{\lambda - u}{u^2} du$$

さてここで，積分範囲が 1 から λ であるが，$\lambda > 1$ と仮定したのであるから，この積分は 0 より大きい．そして，これを $C(\lambda)$ とおいておこう．これは x_i のとりかたによらない定数である．しかし，任意の $\varepsilon > 0$ に対し x_i を十分大きく選べば，

$$\left| \int_{x_i}^{\lambda x_i} \frac{\lambda x_i - t}{t^2} dt \right| = \left| \int_{\lambda x_i}^{\infty} \frac{\lambda x_i - t}{t^2} dt - \int_{x_i}^{\infty} \frac{\lambda x_i - t}{t^2} dt \right| < \varepsilon$$

とできる．しかし $C(\lambda) > 0$ だったから，これは矛盾．反対も同様に示せる．つまり，

$$A(x_i) \leq \lambda x_i$$

となる x_i が無限に存在するように，$\lambda < 1$ を定められたとしよう．そして，

$$\int_{\lambda x_i}^{x_i} \frac{A(t) - t}{t^2} dt$$

について考える．全く同様の計算により，これはある負の定数 $C(\lambda)'$ より小さいことがわかる．これは，

$$\int_1^{\infty} \frac{A(x) - x}{x^2} dx < \infty$$

と矛盾する．

以上の議論から，$x \to \infty$ の時，$A(x) \sim x$ であることがわかる．

続いて，二つ目の補題を紹介する．

補題 2. $f(x)$ を有界な局所可積分関数とする．そして，

$$g(s) = \int_0^{\infty} f(t) e^{-st} dt$$

とおく．すると，$g(s)$ は，$\Re(s) > 0$ で収束し，解析的である．ここで，$g(s)$ を $\Re(s) \geq 0$ に解析接続すると，

$$\int_0^\infty f(t)dt$$

は収束して，その値は $g(0)$ である．

証明は後々やるので，まずはこれを利用した次の定理を紹介する．

定理 3.

$$a_n \geq 0, A(x) = \sum_{n \leq x} a_n$$

とおき，$A(x) = O(x)$ とする．そして，もしディリクレ級数

$$G(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

が $\Re(s) > 1$ において絶対収束して，$\Re(s) \geq 1$ に，一位の極であり，留数 1 を持つ $s = 1$ 以外に解析接続できるとすると，$x \to \infty$ で

$$A(x) \sim x$$

である．

これは，ウィーナー=池原の定理の系である．では証明していこう．

まず，$\Re(s) > 1$ の時，

$$G(s) = s \int_1^\infty \frac{A(x)}{x^{s+1}} dx = \frac{s}{s-1} + s \int_1^\infty \frac{A(x) - x}{x^{s+1}} dx$$
$$\Rightarrow G(s) - \frac{s}{s-1} = s \int_1^\infty \frac{A(t) - t}{t^{s+1}} dt$$

となる．さて，ここで，$G(s)$ の $s = 1$ での留数は 1 だと仮定したのであったから，

$$\lim_{s \to 1} G(s) - \frac{s}{s-1} < \infty$$

となるので，$G(s) - \frac{s}{s-1}$ は $\Re(s) \geq 1$ で解析的である．ここで，s を $s+1$ に置き換えてやると，

$$G(s+1) - \frac{s+1}{s} = (s+1)\int_1^\infty \frac{A(x)-x}{x^{s+2}}dx$$

となり，これの両辺を $s+1$ で割ると，

$$\frac{G(s+1)}{s+1} - \frac{1}{s} = \int_1^\infty \frac{A(x)-x}{x^{s+2}}dx$$

となり，左辺は $\Re(s) \geq 0$ で解析的である．さて，ここで右辺の変数を置換して，$x = e^t$ とおく．すると，

$$\int_1^\infty \frac{A(x)-x}{x^{s+2}}dx = \int_0^\infty \frac{A(e^t)-e^t}{e^{t(s+2)}}e^t dt = \int_0^\infty \left(\frac{A(e^t)-e^t}{e^t}\right)e^{-st}dt$$

ここで，$\left(\frac{A(e^t)-e^t}{e^t}\right)$ は有界で局所可積分である．$A(x), e^t$ が可積分関数なのは明らかだし，これが有界であればよいが，$A(x) = O(x)$ から，これは有界である．よって，補題 2 を適用して，$x = e^t$ とすれば，$dt = \frac{1}{x}dx$ なので，

$$\int_0^\infty \left(\frac{A(e^t)-e^t}{e^t}\right)dt = \int_1^\infty \frac{A(x)-x}{x^2}dx < \infty$$

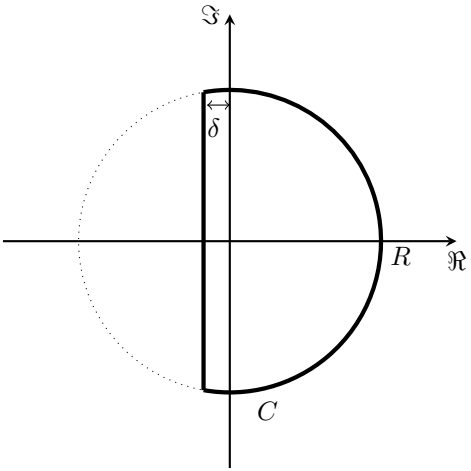
となる．これに補題 1 を適用すれば，

$$A(x) \sim x$$

が言える．よって，この定理は補題 2 を示すことができれば即座に示される．なので，今から補題 2 を示そう．

$$g_T(s) = \int_0^T f(t)e^{-st}dt$$

とすれば，これは積分範囲が有限であるから，整関数になる．そして，



積分路 C を，図の太線部分とする．さて，ここで，

$$\frac{1}{2\pi i}\int_C (g(s)-g_T(s))e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds$$

を考察しよう．まず，δ を十分小さく取れば，C の上と内部で

$$g(s)-g_T(s)$$

を正則にすることが可能である．なぜならば，$g_T(s)$ は整関数であり，$g(s)$ についても，$\Re(s)\geq 0$ で正則なのであるから，虚軸上の各点の近傍で $g(s)$ が正則であるからである．よって，

$$(g(s)-g_T(s))e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)$$

は，$s=0$ に一位の極を持つ以外は C の上と内部で正則である．したがって，留数定理より，この積分は，

$$g(0)-g_T(0)$$

に等しい．ここで

$$\lim_{T\to\infty} g_T(0)=\int_0^\infty f(t)dt$$

だから,

$$\lim_{T\to\infty} g(0) - g_T(0) = 0$$

を示せば目的は達成される．さて，C のうち，円弧である部分の上において，$\sigma = \Re(s), s = Re^{i\theta}$ とおくと,

$$\left| e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)\right| \le e^{\sigma T}\left|\left(\frac{1}{Re^{i\theta}} + \frac{Re^{i\theta}}{R^2}\right)\right| = \frac{e^{\sigma T}}{R}\left|\left(\frac{1}{e^{i\theta}} + e^{i\theta}\right)\right|$$

である．そして,

$$\frac{1}{e^{i\theta}} + e^{i\theta} = e^{-i\theta} + e^{i\theta} = 2\cos\theta = \frac{2\sigma}{R}$$

だから，結局,

$$\left| e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)\right| \le \frac{e^{\sigma T}}{R^2} 2|\sigma|$$

となる．ここで，$f(s)$ は有界であったから，ある定数 M が存在して，$|f(s)| \le M$ になるから，$\sigma > 0$ において,

$$|g(s) - g_T(s)| = \left|\int_T^\infty f(t)e^{-st}dt\right| \le M\left|\int_T^\infty e^{-st}dt\right| \le M\frac{e^{-\sigma T}}{\sigma}$$

となる．したがって，積分路 C の $\Re(s) > 0$ なる部分を C^+ とすれば,

$$\left|\int_{C^+} (g(s) - g_T(s))e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)ds\right| \le \left|\int_{C^+} \frac{e^{\sigma T}}{R^2} 2\sigma M\frac{e^{-\sigma T}}{\sigma}ds\right| = O\left(\frac{1}{R}\right)$$

となる．さて，積分路 C で，$\Re(s) < 0$ で，円弧の一部分となる場所は，δ をいくらでも小さくできることから，考えなくても良い．問題となるのは，積分路のうち縦線部分である．それを V とおいて,

$$\frac{1}{2\pi i}\int_V (g(s) - g_T(s))e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)ds$$

について研究しよう．さて，これは,

$$\frac{1}{2\pi i}\left(\int_V g(s)e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)ds - \int_V g_T(s)e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)ds\right)$$

に等しい．ところで，$g_T(s)$ は整関数であったから，

$$\int_V g_T(s)e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds$$

は積分路 V を図の点線部分，ちょうど C^+ の反対に当たる積分路に変更できる．さてこれを C^- とおこう．ここで，C^- 上で，

$$|g_T(s)| = \left|\int_0^T f(t)e^{-st}dt\right| \leq M\left|\int_0^T e^{-\sigma t}dt\right| \leq M\frac{e^{-\sigma T}}{-\sigma}$$

となるから，

$$\left|e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)\right| \leq \frac{e^{\sigma T}}{R^2}2|\sigma|$$

を思い出すと，

$$\int_V g_T(s)e^{st}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds = O\left(\frac{1}{R}\right)$$

となる．次に，

$$\int_V g(s)e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds$$

について考える．ここで，

$$\int_V g(s)e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds \leq M(R)\int_{-R}^{R} e^{sT}\left(\frac{1}{|s|}+\frac{|s|}{R^2}\right)|ds|$$

となる．（ただし $M(R)$ は，V 上での $g(s)$ の絶対値の最大値.）また，$|e^{sT}| \leq e^{-\delta T}$ より，

$$M(R)\int_{-R}^{R} e^{sT}\left(\frac{1}{|s|}+\frac{|s|}{R^2}\right)|ds| = M(R)e^{-\delta T}\left(O(\log R)+O(1)\right)$$

となる．したがって，

$$\frac{1}{2\pi i}\int_C (g(s)-g_T(s))e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds$$

は，任意の ε に対して，R を十分大きくとって，δ を十分小さくとって，それに対して T_0 を十分大きく取れば，$T_0 \leq T$ なる全ての T において，ε より小さくなる．この積分は $g(0)-g_T(0)$ に等しいのであったから，

$$\lim_{T\to\infty} g(0)-g_T(0) = 0$$

となる．したがって，補題 2 は示された．

8　ウィーナー＝池原の定理の素数定理への適用

さて，いよいよ素数定理の証明である．やはり，鍵となるのは次の数式である．

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

また，

$$\psi(x) = \sum_{n \leq x} \Lambda(n)$$

で，$\psi(x) \sim x$ は素数定理と同値であった．ここで，ウィーナー＝池原の定理を使うために，

$$-\frac{\zeta'(s)}{\zeta(s)}$$

が，留数 1 を持つ一位の極，$s = 1$ を除いて解析的であることを示さなければならない．そのためには，$\Re(s) = 1$ の時，$\zeta(s) \neq 0$ であることが必要である．さて，

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}$$

が $\Re(s) > 1$ で成り立つことを思い出そう．そして，$\Re(s) > 1$ の時，$\zeta(s) \neq 0$ だから，

$$\log \zeta(s) = -\sum_{p} \log \left(1 - \frac{1}{p^s}\right) = \sum_{n,p} \frac{1}{np^{ns}}$$

ここで，$s = \sigma + it$ を代入すると，

$$\log \zeta(\sigma + it) = \sum_{n,p} \frac{1}{np^{n\sigma}} e^{-int \log p}$$

で，$e^{-int \log p}$ の実部は $\cos(nt \log p)$ だから，

$$\log |\zeta(\sigma + it)| = \sum_{n,p} \frac{1}{np^{n\sigma}} \cos(nt \log p)$$

である．そして，少々突飛に思われるかもしれないが，

$$3+4\cos\theta+\cos 2\theta \geq 0$$

を示そう．これは，$\cos 2\theta = 2\cos^2\theta - 1$ を使えば簡単に示せる．

$$\begin{aligned} 3+4\cos\theta+\cos 2\theta &= 3+4\cos\theta+2\cos^2\theta-1 \\ &= 2+4\cos\theta+2\cos^2\theta \\ &= 2(\cos\theta+1)^2 \geq 0 \end{aligned}$$

そして，ここで天下り的であるが，

$$\begin{aligned} &\log|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| \\ =&3\log|\zeta(\sigma)|+4\log|\zeta(\sigma+it)|+\log|\zeta(\sigma+2it)| \\ =&3\sum_{n,p}\frac{1}{np^{n\sigma}}+4\sum_{n,p}\frac{1}{np^{n\sigma}}\cos(nt\log p)+\sum_{n,p}\frac{1}{np^{n\sigma}}\cos(2nt\log p) \\ =&\sum_{n,p}\frac{1}{np^{n\sigma}}(3+4\cos(nt\log p)+\cos(2nt\log p)) \end{aligned}$$

だから，

$$\begin{aligned} &|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| \\ =&\exp\left(\sum_{n,p}\frac{1}{np^{n\sigma}}(3+4\cos(nt\log p)+\cos(2nt\log p))\right) \geq 1 \end{aligned}$$

が $\sigma > 1$ で成り立つ．さてここで両辺を $\sigma - 1$ で割って，明らかな変換をすると，

$$|(\sigma-1)\zeta(\sigma)|^3\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^4|\zeta(\sigma+2it)| \geq \frac{1}{\sigma-1} \tag{6}$$

となる．そして，$\zeta(s)$ を $\Re(s) > 0$ に解析接続したときのことを思い出そう．

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt$$

これは，$s=1$ で一位の極を持ち，その留数は 1 であった．さて (6) で $\zeta(1+it)=0$ と仮定して，$\sigma \to 1+$ の極限を考えよう．すると，左辺は，

$$|\zeta'(1+it)|^4|\zeta(1+2it)|$$

となって，有限値になる．しかし，右辺は明らかに無限大に発散するから，これは矛盾．したがって，$\Re(s)=1$ の時，$\zeta(s)\neq 0$.

ここで，$\zeta(s)$ は，$\Re(s)>0$ で，留数 1 を持つ一位の極，$s=1$ 以外に極を持たなかった．したがって，$-\zeta'(s)/\zeta(s)$ も留数 1 を持つ一位の極，$s=1$ 以外に極を持たない．なぜならば，

$$\begin{aligned}
-(s-1)\frac{\zeta'(s)}{\zeta(s)} &= -(s-1)\frac{\frac{-1}{(s-1)^2}+a_1+a_2(s-1)+\dots}{\frac{1}{s-1}+a_0+a_1(s-1)+\dots} \\
&= \frac{\frac{1}{s-1}-a_1(s-1)-a_2(s-1)^2-\dots}{\frac{1}{s-1}+a_0+a_1(s-1)+\dots} \\
&= \frac{1-a_1(s-1)^2-a_2(s-1)^3-\dots}{1+a_0(s-1)+a_1(s-1)^2+\dots}
\end{aligned}$$

となり，ここで $s\to 1$ とすれば，

$$\lim_{s\to 1} -(s-1)\frac{\zeta'(s)}{\zeta(s)} = 1$$

となるからである．これは，定理 3 の条件を満たしている．つまり，

$$\sum_{n\leq x}\Lambda(n)=\psi(x)\sim x$$

が $x\to\infty$ で成り立つ．したがって，

定理 4.

$$\pi(x)\sim\frac{x}{\log x}$$

9　ウィーナー＝池原の定理の拡張

定理 3 は，それだけで十分強力な定理であるが，さらに拡張することが可能である．次の点について考えていこう．ただし，文中の「ウィーナー＝池原の

定理」はその前の項目での結果も含めて使えることとする.

1. もし留数が $R > 0$ の時,

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n/R}{n^s}$$

を考える．すると，$f(s)$ の $s = 1$ での留数は 1 になる．よって,

$$\sum_{n \leq x} a_n = Rx + o(x)$$

2. もし留数が $R = 0$ の時，これは極を持たないことと同じだが，ここで

$$f(s) + \zeta(s)$$

を考える．すると定理 3 が適用できて,

$$\sum_{n \leq x} (a_n + 1) = x + o(x)$$

となるから,

$$\sum_{n \leq x} a_n = o(x)$$

となる.

3. さてここで，$a_n \geq 0$ という制約を外すことを試みる.

$$g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}, b_n \in \mathbb{R}$$

とおく．そして，$g(s)$ が $\Re(s) > 1$ で絶対収束して，$\Re(s) \geq 0$ の，一位の極で，留数 r を持つ $s = 1$ 以外の領域に解析接続できるとしよう．すると，定理の条件を満たして，$|b_n| \leq a_n$ となる $a_n \geq 0$ が存在して，$x \to \infty$ の時,

$$\sum_{n \leq x} b_n = rx + o(x)$$

となる．これを示そう．まず，

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

として，$f(s) - g(s)$ にウィーナー=池原の定理を適用しよう．すると，

$$\sum_{n \leq x} (a_n - b_n) = (R - r)x + o(x)$$

となる．あとは明らかであろう．

4. 今度は，これを複素数にまで拡張したい．つまり，$b_n \in \mathbb{R}$ から $b_n \in \mathbb{C}$ に制限を緩めたい．まず，$f(s)$ が $\Re(s) \geq 1$ で解析的ならば，

$$\overline{f(\overline{s})}$$

も解析的である．これは，コーシー・リーマンの方程式から導くことができる．$f(s) = f(x + yi) = u(x, y) + iv(x, y)$ が $\Re(s) \geq 1$ で解析的なのだから，

$$u_x(x, y) = v_y(x, y), v_x(x, y) = -u_y(x, y)$$

が成り立つ．ここで，$\overline{f(\overline{s})} = u(x, -y) - iv(x, -y)$ だから，$\overline{u}(x, y) = u(x, -y), \overline{v}(x, y) = -v(x, -y)$ とすれば，

$$\overline{u}_x(x, y) = u_x(x, -y), \overline{u}_y(x, y) = -u_y(x, -y)$$
$$\overline{v}_x(x, y) = -v_x(x, -y), \overline{v}_y(x, y) = v_y(x, -y)$$

だから，

$$\overline{u}_x(x, y) = \overline{v}_y(x, y), \overline{v}_x(x, y) = -\overline{u}_y(x, y)$$

が $\Re(s) \geq 1$ で成り立つので，この領域において，$\overline{f(\overline{s})}$ は解析的である．さて，ここで，

$$g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

として，これが $\Re(s) > 0$ で絶対収束して，$\Re \geq 0$ に解析接続した時，留数 R を持つ，$s = 1$ 以外に極を持たないとしよう．そして，$\overline{g(\overline{s})}$ を考える．これは，

$$\overline{g(\overline{s})} = \overline{\sum_{n=1}^{\infty} \frac{b_n}{n^{\overline{s}}}} = \sum_{n=1}^{\infty} \frac{\overline{b_n}}{n^s}$$

である．そして，これを $g^*(s)$ とおこう．すると，

$$\sum_{n=1}^{\infty} \frac{\Re(b_n)}{n^s} = \frac{g(s) + g^*(s)}{2}, \sum_{n=1}^{\infty} \frac{\Im(b_n)}{n^s} = \frac{g(s) - g^*(s)}{2i}$$

となる．したがって，ウィーナー=池原の定理から，

$$\sum_{n \leq x} \Re(b_n) = \Re(R)x + o(x), \sum_{n \leq x} \Im(b_n) = \Im(R)x + o(x)$$

となるから，

$$\sum_{n \leq x} b_n = Rx + o(x)$$

が，$b_n \in \mathbb{C}$ においても成り立つ．

では，これまでの結果をまとめよう．

定理 5.

$$a_n \in \mathbb{C}, A(x) = \sum_{n \leq x} a_n$$

とおく．そして，もしディリクレ級数

$$G(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

が $\Re(s) > 1$ において絶対収束して，$\Re(s) \geq 1$ に，一位の極であり，留数 R を持つ $s = 1$ 以外に解析接続できるとすると，$x \to \infty$ で

$$A(x) = Rx + o(x)$$

である．

10　ウィーナー＝池原の定理の応用

ウィーナー＝池原の定理は応用の広い定理である．ここではその応用を，素数定理以外にもうひとつ紹介する．

10.1　多冪数

n が多冪数（squarefull）であるとは，全ての素数について，$p|n \Rightarrow p^2|n$ が成り立つことである．例えば，12 は多冪数ではない．なぜなら，3 で割り切れるが，$3^2 = 9$ では割り切れないからである．しかし，$72 = 2^3 3^2$ などは多冪数である．さて，a_n を，

$$a_n = \begin{cases} 1, & n\,is\,squarefull \\ 0 & otherwise \end{cases}$$

として，ディリクレ級数

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

を考えよう．そして，ここで注目すべきは，a_n は乗法的関数になっているということである．つまり，$(n, m) = 1 \Rightarrow a_n a_m = a_{nm}$ が成り立つ．したがって，

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \left(1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \dots\right) = \prod_p \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots\right)$$

となる．ここで，

$$\begin{aligned} 1 + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots &= 1 + \frac{1}{p^{2s}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) \\ &= 1 + \frac{1}{p^{2s}\left(1 - \frac{1}{p^s}\right)} \\ &= 1 + \frac{1}{p^s(p^s - 1)} \end{aligned}$$

そして,

$$1+\frac{1}{p^s(p^s-1)}=\frac{p^{2s}-p^s+1}{p^s(p^s-1)}=\frac{p^{3s}+1}{p^s+1}\cdot\frac{1}{p^s(p^s-1)}=\frac{p^{3s}+1}{p^{2s}-1}\cdot\frac{1}{p^s}$$

となり，分母と分子を両方 p^{3s} で割れば,

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

となる．だから,

$$f(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}=\prod_p\left(1+\frac{1}{p^{3s}}\right)\left(1-\frac{1}{p^{2s}}\right)^{-1}$$

となる．さて，ここで,

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}$$

だったことを思い出そう．すると,

$$f(s)=\prod_p\left(1+\frac{1}{p^{3s}}\right)\left(1-\frac{1}{p^{2s}}\right)^{-1}=\zeta(2s)\prod_p\left(1+\frac{1}{p^{3s}}\right)$$

となる．また，$(1-x^6)/(1-x^3)=1+x^3$ より,

$$\zeta(2s)\prod_p\left(1+\frac{1}{p^{3s}}\right)=\zeta(2s)\prod_p\left(\frac{1-\frac{1}{p^{6s}}}{1-\frac{1}{p^{3s}}}\right)=\frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

まとめると,

$$f(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}=\frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

となる．さてこれを $\Re(s)\geq 1/2$ まで解析接続しよう．すると，これは $s=1/2$ に一位の極を持つ．問題になるのはその留数だが,

$$\lim_{s\to\frac{1}{2}}\left(s-\frac{1}{2}\right)\frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}=\lim_{s\to\frac{1}{2}}\frac{1}{2}\frac{(2s-1)\zeta(2s)\zeta(3s)}{\zeta(6s)}=\frac{\zeta(3/2)}{2\zeta(3)}$$

である．さてここで，ウィーナー=池原の定理を使うと，

$$\sum_{n\leq x} a_n \sim \frac{\zeta(3/2)}{2\zeta(3)} x^{\frac{1}{2}}$$

となる．　なぜ $x^{\frac{1}{2}}$ になっているかというと，解析接続した範囲が $\Re(s) \geq 1/2$ だからである．要するに，$\Re(s) > \theta$ でディリクレ級数が絶対収束して，$s = \theta$ に留数 R を持つ極があって，$\Re(s) = \theta$ にはそれ以外極がないとすると，そのディリクレ級数の定義から，

$$G(s-(1-\theta)) = \sum_{n=1}^{\infty} \frac{a_n}{n^{s-(1-\theta)}} = \sum_{n=1}^{\infty} \frac{a_n n^{1-\theta}}{n^s}$$

となるから，となって，これはウィーナー=池原の定理が使える形である．すなわち，

$$\sum_{n\leq x} a_n n^{1-\theta} = Rx + o(x)$$

となる．ここで，左辺の和にアーベルの総和法を適用すれば，

$$\sum_{n\leq x} a_n n^{1-\theta} = A(x)x^{1-\theta} - (1-\theta)\int_1^x \frac{A(t)}{t^\theta} dt$$

よって，

$$A(x) - \frac{1-\theta}{x^{1-\theta}} \int_1^x \frac{A(t)}{t^\theta} dt = Rx^\theta + o(x^\theta)$$

となり，また $G(s)$ は，$\Re(s) > \theta$ で絶対収束するのだから，$A(x) = O(x^{\theta-1})$ である．よって，左辺の積分は $O(x^{\theta-1}\log x)$ となり，$o(x^\theta)$ であるから，結局，

$$A(x) \sim Rx^\theta$$

となる．ここで本題に戻ると，結局，x 以下の多冪数の数は

$$\frac{\zeta(3/2)}{2\zeta(3)} x^{\frac{1}{2}}$$

に漸近するという公式が得られる．

11　算術級数中の素数

11.1　指標について

まず，$(\mathbb{Z}/p\mathbb{Z})^*$ について説明する[10]．これは何かというと，これは，$\mathbb{Z}/p\mathbb{Z}$ のうち，p と互いに素な剰余類を集めた物である．さて記号を説明するのにさらに分からない記号を増やしてしまった．順に説明していこう．（q を法とする）a の剰余類とは，

$$\overline{a} = \{k \mid k \equiv a \pmod{q}\}$$

なる集合 $\overline{a}$ である．そして，$\mathbb{Z}/q\mathbb{Z}$ とは，q を法とした剰余類を全て集めた集合である．しかしながら，$\overline{a} = \overline{a+q}$ であることから，$\mathbb{Z}/q\mathbb{Z}$ は無限集合とはならない．例えば，$\mathbb{Z}/5\mathbb{Z}$ について考えると，

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

となる．一般に，

$$\mathbb{Z}/q\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{q-1}\}$$

である．そして，$(\mathbb{Z}/p\mathbb{Z})^*$ は，前述の通り p と互いに素な剰余類を全て集めた集合である．このような剰余類は $\mathbb{Z}/p\mathbb{Z}$ に含まれる $\overline{0}$ 以外の全ての剰余類である．よって例えば素数 p に対して，

$$(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

となる．

さてここで，G をアーベル群として，写像 $f : G \mapsto \mathbb{C}\backslash\{0\}$ は，準同型である時，つまり，任意の $g_1, g_2 \in G$ に対して，$f(g_1g_2) = f(g_1)f(g_2)$ が成り立つとき，G の指標と呼ばれる．各 $f(g)$ の値は 1 の冪根である．なぜならば，任意の

[10] この節の解説は，tsujimotter 氏の「群論におけるフェルマーの小定理」を大いに参考にした．http://tsujimotter.hatenablog.com/entry/fermat-little-theorem-by-group-theory（最終閲覧日：2019/8/19）

$g \in G$ に対して $n \in \mathbb{N}$ が存在して，$g^n = e$ とでき，$f(g)^k = f(g^k) = f(e) = 1$ となるからである．

11.1.1 ディリクレ指標

本稿で問題になるのは主にディリクレ指標であるから，それについて解説する．ディリクレ指標とは，ある整数 q に対して，

- $a \equiv b \pmod{q}$ ならば，$\chi(a) = \chi(b)$.
- $\chi(ab) = \chi(a)\chi(b)$
- $\chi(1) = 1$
- $(a, q) \neq 1$ ならば，$\chi(a) = 0$

という性質を持つ関数 χ である．これは実際には指標ではないのだが，指標を拡張したものと捉えられるので，指標と呼ばれる．

これからディリクレ指標を構成するが，まず，$(\mathbb{Z}/q\mathbb{Z})^*$ が巡回群となる場合は簡単である．つまり，$(\mathbb{Z}/q\mathbb{Z})^*$ の元が全て一つの元，g の冪で表現される場合，$\chi(g) = \zeta$（ただし ζ は 1 の冪根）とすれば，これは $(\mathbb{Z}/q\mathbb{Z})^*$ の元全てに対して χ の値を与える．なぜなら，χ は定義から完全乗法的関数だから，$\chi(g^k) = \chi(g)^k$ となって，k の値を様々に取れば，g^k が $(\mathbb{Z}/q\mathbb{Z})^*$ の全ての元をわたるからだ．ちなみに，この g を法 q に対する原始根，という．さて，この原始根がいつでも存在すればいいのだが，そうとはいかない．なので，場合分けをして考えよう．

q が素数の場合 q が素数の場合は原始根が必ず存在する．この場合はその原始根 g に対して，1 の $q-1$ 乗根を適当に選んで $\chi(g)$ にすれば良いのであった．したがって，ディリクレ指標は $q - 1 = \varphi(q)$ 個あるはずである．ここで，q が素数の場合，必ず原始根があることを示そう[11]．

[11] この証明は，高木貞治「初等整数論講義」によった．

まず，a を q で割り切れない数として，a は m 乗して初めて $a^m \equiv 1 \pmod{q}$ になるとしよう．ここで，$(a^k)^m = (a^m)^k \equiv 1 \pmod{q}$ より，$a^0(=1), a^1, \ldots, a^{m-1}$ は全て $x^m \equiv 1 \pmod{q}$ の解であるが，これらは全て互いに合同でない．よって，これが $x^m \equiv 1 \pmod{q}$ の全ての解である．これは，q が素数だから成り立つ．

今からこれを示す．p が素数な時は，$f(x) \equiv 0 \pmod{p}$ の解の一つを a とすると，代数的変換によって，$f(x) = (x-a)f_1(x) + f(a)$ とできる．ここで f_1 は a_0x^{n-1} を最高次とする整数係数多項式である．(これは一次方程式をといて係数を決定していけるので，必ず存在する.）すると，方程式は $(x-a)f_1(x) \equiv 0$ と同一の解を持つ．ここで $n-1$ 次の方程式に対して，高々$n-1$ 個の解しかないことが分かっていれば，これは数学的帰納法により示される．ここで，$a_0x + a_1 \equiv 0 \pmod{p}$ は p を法としてただ一つの解を持つ．なぜなら，$1, 2, \ldots, p-1$ に a_0 をかけた $a_0, 2a_0, \ldots, (p-1)a_0$ を p で割ったあまりがかぶることはないから[12]，ただ一つに定まるからである．これらの議論から，素数 p を法とした n 次の合同方程式は高々n 個の解しか持たない．

さて，本題に戻ろう．$m = \varphi(q) = q-1$ ならば a 自体が原始根である．そうでない場合，もっと大きな指数に対応する数が必ず求められることを示そう．そうすれば，最終的に $q-1$ に達する．さて，$m < q-1$ ならば，$a^0, a^1, \ldots, a^{m-1}$ と合同でない整数が存在する．仮にそれを b とおく．そして，b は指数 $n > 1$ に対応するものとする.（つまり n 乗して初めて 1 と合同になる.）

1. $(m, n) = 1$ の時：

   まず，$(ab)^{mn} = a^m b^n \equiv 1^m 1^n \equiv 1 \pmod{q}$ である.，反対に，$(ab)^x \equiv 1 \pmod{q}$ とすれば，$(ab)^{xm} \equiv 1 \pmod{q}$ で，仮定に

[12] 本稿の乗法的関数の項をみよ

よって $a^m \equiv 1$ だから，$b^{xm} \equiv 1$ となる．よって，$n|x$ である．同様にして，$m|x$ であるから，x は m, n の公倍数．したがってこれは最小公倍数 mn の倍数．だから，ab は指数 mn に対応する．したがって，ab は m より大きい指数に対応する．

2. $(m, n) = d > 1$ の時：

   m, n の最小公倍数を l とする時，$l = mn/d = m_0 n_0$ として，$(m_0, n_0) = 1, m_0|m, n_0|n$ とできる．そして,，a^{m/m_0} は指数 m_0 に対応し，b^{n/n_0} は指数 n_0 に対応する．ここで，1 の結果から，$a^{m/m_0} b^{n/n_0}$ は指数 $m_0 n_0 = l$ に対応する．ここで，l が m でない，つまり n が m の約数でないことを示す．もし n が m の約数と仮定すると，$b^m \equiv 1 \pmod{q}$ となってしまい，$a^0, a^1, \ldots, a^{m-1}$ が $x^m \equiv 1 \pmod{q}$ の全ての解なのだから，これは b の仮定に反する．

これらを組み合わせると，a が指数 $m < q - 1$ に対応している時，もっと大きい指数に対応する数が存在する．よって，原始根は q が素数の時必ず存在する．

q が奇素数 p の冪の時 q が奇素数 p の時の結果を利用して，奇素数 p の冪の場合において考えよう[13]．p^k を法とした原始根があることを示せば良い．g を p を法とした原始根としよう．そして，

$$(g + pt)^{p-1} \not\equiv 1 \pmod{p^2}$$

なる t を探そう．$g^{p-1} \not\equiv 1 \pmod{p^2}$ ならば $t = 0$ を取れば良い．そうでないなら，

$$\begin{aligned}(g + pt)^{p-1} &\equiv g^{p-1} + \binom{p-1}{1} g^{p-2} pt \\ &\equiv 1 + p(p-1) t g^{p-2} \pmod{p^2}\end{aligned}$$

[13] Ram Murty,「Problems in analytic number theory」を参考にした．また，この本はこれからの 3 つにおいて，ほぼ丸々引用している．

となって，$t=1$ とすれば条件を満たす．さてここで，p^α を法として，$g+pt$ が位数 d を持つとしよう[14]．すると，$d|\varphi(p^\alpha)=p^{\alpha-1}(p-1)$ となる，また，g は p を法とした原始根なのだから，$(p-1)|d$ である．したがって，$r\leq a$ なる r があって，$d=p^{r-1}(p-1)$ となる．さてここで，$(g+pt)^{p-1}\not\equiv 1 \pmod{p^2}$ の仮定から，$(g+pt)^{p-1}=1+pu_1, p\not| u_1$ となる．したがって，

$$\begin{aligned}(g+pt)^{p(p-1)} &= (1+pu_1)^p \\ &= 1+\binom{p}{1}pu_1+\binom{p}{2}(pu_1)^2+\dots\end{aligned}$$

ここで，p が奇数だから，$\binom{p}{2}=p(p-1)/2\equiv 0 \pmod{p}$．したがって，$p^3$ を法として考えると，3 項目以降が消えて，

$$(g+pt)^{p(p-1)}\equiv 1+p^2u_1 \pmod{p^3}$$

この操作を繰り返すと，

$$(g+pt)^{p^{b-1}(p-1)}\equiv 1+p^bu_1 \pmod{p^{b+1}}$$

となる．今，$g+pt$ は p^α を法として位数 $d=p^{r-1}(p-1)$ を持つ．

$$(g+pt)^{p^{r-1}(p-1)}\equiv 1 \pmod{p^\alpha}$$

その時，$r+1\leq\alpha$ とすると，$1\equiv(g+pt)^{p^{r-1}(p-1)} \pmod{p^{r+1}}$ ともなる[15]．しかし，$(g+pt)^{p^{r-1}(p-1)}\equiv 1+p^ru_1 \pmod{p^{r+1}}$ であった．したがって，$1\equiv 1+p^ru_1 \pmod{p^{r+1}}$ となる．よって，u_1 が p で割り切れてしまう．これは矛盾．したがって $r=\alpha$ となって目的は達せられた．

q が 2 の冪の時 $2,4$ の場合は，それぞれ原始根が存在する（それぞれ $1,3$）．

したがって $q=2^\alpha, \alpha>2$ の場合を考える．次の項目でディリクレ指標

[14] 位数とは，何回目の冪で 1 になるかの数である．さっき,「対応する」と書いていたのがこれ．

[15] $(g+pt)^{p^{r-1}(p-1)}$ は a 以下の p の冪を法としても 1 になるから

を構成するから，この項目ではそれの準備をしよう．まず，5 の 2^α に対する位数を考えていく．5 の 2^α に対する位数は，$2^{\alpha-2}$ である．これは，

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$$

を示すことで証明できる．$5 \equiv 1 + 4 \pmod{2^3}$ だから，$n = 3$ の時は明らかである．ここで，n の時成り立つとすると，当然

$$5^{2^{n-3}} = 1 + 2^{n-1} + 2^n u$$

となる．ここで，

$$\begin{aligned} 5^{2^{n-2}} &= (1 + 2^{n-1} + 2^n u)^2 \\ &= 1 + 2(2^{n-1} + 2^n u) + (2^{n-1} + 2^n u)^2 \\ &= 1 + 2^n + 2^{n+1} u + 2^{2n-2} + 2^{2n} u + 2^{2n} u^2 \\ &= 1 + 2^n + 2^{n+1}(u + 2^{n-3} + 2^{n-1} u + 2^{n-1} u^2) \end{aligned}$$

となるから $n + 1$ についても成り立つ．数学的帰納法によって，$n > 2$ の全ての n について成り立つ．ここで，

$$5^{2^{\alpha-2}} \equiv (1 + 2^{\alpha-1})^2 \equiv 1 \pmod{2^\alpha}$$

となるから，5 の 2^α に対する位数は，$2^{\alpha-2}$ である．これより小さいのではないか，と思われるかもしれないが r が位数だとすると，$5^r \equiv 1 \pmod{2^{\alpha-1}}$ でもなくてはならないから $2^{\alpha-3}$ の倍数である必要がある．それを考えると，$2^{\alpha-2}$ が最小である．

さてここで，$(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ が，$\alpha \geq 3$ の時，$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ と同型であることを示そう．まず群 G, H が同型であるとは，$f(g_1 g_2) = f(g_1) f(g_2)$ が全ての $g_1, g_2 \in G$ について成り立つような写像 (準同型写像) で，かつその逆写像も準同型写像であるような写像が存在する，ということである．これを $G \cong H$ と書くこともある．さて，$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$

を実際に写像を構成していくことで示していこう． まず $\alpha \geq 3$ の時,, $5^j \not\equiv -1 \pmod{2^\alpha}$ ということを確認しよう．これは 4 を法として考えた時，$5^j \equiv 1 \equiv -1 \pmod 4$ となるのは矛盾だからである．さて，法 2^α において，5 の位数は $2^{\alpha-2}$ であった．したがって , $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ の元は，$\overline{\pm 5^j}$ の形で表される．例えば $\alpha = 3$ とすると，$\overline{1}, \overline{5}$ は $\overline{+5^j}$ で表される物，それ以外は $\overline{-5^j}$ で表される物である．さてここで，$(\mathbb{Z}/2\mathbb{Z})$ の元として符号を，つまり，$\overline{+5^j}$ で表されるものには $\overline{0}$，$\overline{-5^j}$ で表されるものには $\overline{1}$，を対応させ，$(\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ の元として，$\overline{\pm 5^j}$ の形で表される物に対して $\overline{j}$ を対応させる写像を考えると，これは $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ から $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ への準同型写像になっている．これを確認するのは容易である．例えば，$(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ の元として，$\overline{+5^j}, \overline{+5^k}$ をとってくると，これらを掛け合わせたものは $\overline{+5^{j+k}}$ となるから，これは条件を満たす．これ以外も容易に確かめられる．さて準同型写像であることは良いとして，これが同型写像であることを示したい．しかし，この写像は一対一対応，つまり全単射だから，それはもう果たされているのである．今それを示そう[16]．$\varphi : G \mapsto H$ が準同型写像で，それが全単射だとする．G, H の単位元をそれぞれ $1_G, 1_H$ と表記すると，逆写像 ψ を考えた時，$\varphi(1_G) = 1_H$ だから，$\psi(1_H) = 1_G$ となる．また，$a, b \in H$ とすると，

$$\varphi(\psi(ab)) = ab = \varphi(\psi(a))\varphi(\psi(b)) = \varphi(\psi(a)\psi(b))$$

となって，$\psi(ab) = \psi(a)\psi(b)$ となる．したがって逆写像も準同型写像であるから，これは同型写像である．この結果を利用することで，先の写像が同型写像であることがわかる．

その他の場合 $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ と素因数分解されているとする．すると，これが

$$(\mathbb{Z}/q\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^* \times \dots (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*$$

[16]証明は雪江明彦「整数論 1」によった.

となることはわかりやすいであろう．さてここで，$(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ それぞれからディリクレ指標を取り出して

$$\chi = \chi_1\chi_2\cdots\chi_k$$

として，χ を $(\mathbb{Z}/q\mathbb{Z})^*$ のディリクレ指標とする．ここで，$\chi_1\chi_2$ というのは，$(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$ となるような関数である．これからわかる通り，これもまたディリクレ指標となっている．群の他の条件も満たすので，ディリクレ指標はこの演算に対して群をなす．さて，χ の選び方の総数を知りたいのだが，これは $\chi_1, \chi_2, \ldots, \chi_k$ の k 個のディリクレ指標の選び方の組み合わせの総数に等しい．ここで

1. $p_i \neq 2$ の時，$(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ は巡回群となるのだったから，選び方の総数は $\varphi(p_i^{\alpha_i})$ である．
2. $p_i = 2$ の時，$(\mathbb{Z}/2^{\alpha_i}\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha_i-2}\mathbb{Z})$ はだったから，選び方の総数は $2\cdot 2^{\alpha_i-2} = 2^{\alpha_i-1} = \varphi(2_i^{\alpha})$ である．これらをまとめると，選び方の総数は，

$$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k}) = \varphi(q)$$

となって，q を法としたディリクレ指標の選び方は $\varphi(q)$ 個であり，ディリクレ指標の指標群の位数も $\varphi(q)$ である．

11.2 ディリクレの L 関数

ディリクレの L 関数を以下のように定義する．

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

ただし，χ はディリクレ指標とする．これもまたディリクレ級数である．さてここで，$\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ を思い出そう．要するにこれは χ が完全乗法

的関数ということを意味している．したがって，ディリクレの L 関数はオイラー積の形にかけて，

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

となる．χ が完全乗法的関数なので，このようにシンプルに書けるのである．

11.2.1 ディリクレ指標の性質

さて，この L 関数の性質を調べるために有用な直交関係式と呼ばれるものを紹介しておこう．一つ目は

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(q) & a\equiv 1 \pmod q\\ 0 & otherwise\end{cases}$$

が成り立つというものである．ここで和は全てのディリクレ指標をわたる．さてこれを証明しよう．

まず，$a\equiv 1 \pmod q$ となる場合はいいだろう．全てのディリクレ指標に対して，$\chi(a)=1$ となって，それが $\varphi(q)$ 個足し合わされるからだ．問題は $a\not\equiv 1 \pmod q$ となる場合である．ここで，$\chi_1(a)\neq 1$ となるようにディリクレ指標を選んでこよう．これは，$a\not\equiv 1 \pmod q$ だから必ず一つは存在する．さてここで，

$$\chi_1(a)\sum_{\chi}\chi(a)=\sum_{\chi}(\chi_1\chi)(a)$$

について考えよう．ここで，ディリクレ指標は群をなすから，$\chi_1\chi$ はまたディリクレ指標になる．そして，χ を様々に動かせば $\chi_1\chi$ は全てのディリクレ指標をわたる．なぜなら，もし $\chi_1\chi_2=\chi_1\chi_3$ とすれば，全ての a について，$\chi_2(a)=\chi_3(a)$ となってしまうから，$\chi_2=\chi_3$ となるからである．さて，この議論から，

$$\chi_1(a)\sum_{\chi}\chi(a)=\sum_{\chi}\chi(a)$$

がわかる．$\chi_1(a) \neq 1$ としたのだから，

$$\sum_{\chi} \chi(a) = 0$$

となる．さて今度は，ディリクレ指標ではなく a を様々にかえた物を考えてみよう．

$$\sum_{(a,q)=1} \chi(a) = \begin{cases} \varphi(q) & \chi = \chi_0 \\ 0 & otherwise \end{cases}$$

ここで，χ_0 とは自明なディリクレ指標，つまり，全ての $(a,q) = 1$ なる a について，$\chi(a) = 1$ となるディリクレ指標である．この場合は，当然 $\varphi(q)$ になる．問題はディリクレ指標が自明でない場合だが，これは前と同様に示すことができる．つまり，自明でないディリクレ指標なのだから，$\chi(b) \neq 1, (b,q) = 1$ となるような b が絶対に存在する．そして，

$$\chi(b) \sum_{(a,q)=1} \chi(a) = \sum_{(a,q)=1} \chi(ab) = \sum_{(a,q)=1} \chi(a)$$

だから

$$\sum_{(a,q)=1} \chi(a) = 0$$

となる．

11.2.2 L 関数の部分和

さて，ここで，非自明なディリクレ指標 χ に対して，

$$\sum_{n \leq q} \chi(n) = 0$$

が成り立つことに注意しよう．なぜなら，$(a,q) \neq 1$ なる a に対しては，$\chi(a) = 0$ だからである．ここで，L 関数は，

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

と定義されたのであった．これの部分和，つまり，

$$\sum_{n\leq x}\frac{\chi(n)}{n^s}$$

について考えてみよう．χ を非自明なディリクレ指標として，

$$S(x)=\sum_{n\leq x}\chi(n)$$

とおくと，アーベルの総和法を用いて，

$$\sum_{n\leq x}\frac{\chi(n)}{n^s}=\frac{S(x)}{x^s}+s\int_1^x\frac{S(x)}{x^{s+1}}dx$$

となる．さてここで，$|S(x)|<q$ になることは，

$$\sum_{kq<n\leq(k+1)q}\chi(n)=0$$

が成り立つことから容易にわかる．したがって，$x\to\infty$ を考えると，少なくとも $\Re(s)>0$ の領域において，

$$L(s,\chi)=s\int_1^\infty\frac{S(x)}{x^{s+1}}dx$$

が成り立つ．そして，積分は $\Re(s)>0$ の時収束するから，$\chi\neq\chi_0$ の時，

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

は $\Re(s)>0$ で収束して，解析関数になる．$\chi=\chi_0$ の時はオイラー積表示を考えると良い．つまり，

$$L(s,\chi)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

で素数 p が q を割り切る時のみ，$(p,q)\neq1$ で $\chi(p)=0$，それ以外の場合は $\chi(p)=1$ だから，p が q を割り切る時以外,，ゼータ関数のオイラー積表示と同じである．すなわち，

$$L(s,\chi)=\zeta(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right)$$

となる．これは，一位の極，$s=1$ を除いて $\Re(s)>0$ で解析的である．また，$s=1$ での留数は，

$$\lim_{s\to 1}(s-1)\zeta(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right)=\prod_{p|q}\left(1-\frac{1}{p}\right)=\frac{\varphi(q)}{q}$$

となる．

11.3 算術級数中の素数とディリクレ L 関数

さて，ゼータ関数の時と同じように，L 関数の対数微分を考えてみよう．

$$\log L(s,\chi)=-\sum_{p}\log\left(1-\frac{\chi(p)}{p^s}\right)=\sum_{p\ prime,n\geq 1}\frac{\chi(p)^n}{np^{ns}}$$

項別微分すると，

$$-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{p\ prime,n\geq 1}\frac{\chi(p)^n\log p}{p^{ns}}=\sum_{m=1}^{\infty}\frac{\chi(m)\Lambda(m)}{m^s}$$

となる．ここで，全ての指標について，これを足し合わせてみよう．

$$\sum_{\chi}-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{m=1}^{\infty}\frac{\Lambda(m)}{m^s}\sum_{\chi}\chi(m)$$

が $\Re(s)>1$ において成り立つ．さて，ここで，

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(q) & a\equiv 1 \pmod q\\ 0 & otherwise\end{cases}$$

を思い出そう．すると，

$$\sum_{\chi}-\frac{L'(s,\chi)}{L(s,\chi)}=\varphi(q)\sum_{n\equiv 1 \bmod q}\frac{\Lambda(n)}{n^s}$$

そして，$\Re(s)=1$ の時，

$$L(s,\chi)\neq 0$$

と仮定しよう．これは大きな仮定であるが，ゼータ関数の時と同じように証明できると想像できる．さてこの仮定を用いると，ウィーナー＝池原の定理から，

$$\varphi(q) \sum_{\substack{n\equiv 1 \bmod q \\ n\leq x}} \Lambda(n) \sim x$$

が成り立つ．さて，ここで，$\Lambda(m)$ は p の冪に対しても $\log p$ を返すのであったが，それらが全体に及ぼす影響は非常に小さいのであった[17]．よってこれは以下のように書き換えられる．

$$\varphi(q) \sum_{\substack{p\equiv 1 \bmod q \\ p\leq x}} \log(p) \sim x$$

よって，以下の漸近式を得る．

$$\sum_{\substack{p\equiv 1 \bmod q \\ p\leq x}} \log(p) \sim \frac{x}{\varphi(q)}$$

したがって，ここから $p \equiv 1 \pmod q$ なる素数 p が無限に存在することがわかり，それの数を評価する式を得た．しかし，無限に存在すること自体はは初等的な方法でも示せる[18]からそこまでの驚きはないだろう．この 1 を一般の a にしたいのであるが，どうすれば良いだろうか． まず，

$$\sum_{\chi} -\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{m=1}^{\infty} \frac{\Lambda(m)}{m^s} \sum_{\chi} \chi(m)$$

に戻って考える．左辺を，

$$\sum_{\chi} \overline{\chi(a)} \left(-\frac{L'(s,\chi)}{L(s,\chi)} \right)$$

に変えてみよう．すると，

$$\sum_{\chi} \overline{\chi(a)} \left(-\frac{L'(s,\chi)}{L(s,\chi)} \right) = \sum_{m=1}^{\infty} \frac{\Lambda(m)}{m^s} \sum_{\chi} \overline{\chi(a)}\chi(m)$$

[17]詳しくは本稿の 4.2 節を見よ．
[18]高木貞治「初等整数論講義」p56 等を見よ．

となる．ここで，$\overline{\chi(a)} = \chi(a^{-1})$ である．ここで a^{-1} というのは q を法として考えるのである．つまり，$at \equiv 1 \pmod{q}$ なる t である．これは，$(a, q) = 1$ ならば必ず存在する．すると，

$$\overline{\chi(a)}\chi(m) = \chi(a^{-1})\chi(m) = \chi(a^{-1}m)$$

となる．ここで $a^{-1}m \equiv 1$ は，両辺に a をかけると，$m \equiv a$ になるから，

$$\sum_{\chi} \overline{\chi(a)} \left(-\frac{L'(s,\chi)}{L(s,\chi)} \right) = \varphi(q) \sum_{n \equiv a \bmod q} \frac{\Lambda(n)}{n^s}$$

となって，

$$\varphi(q) \sum_{\substack{p \equiv a \bmod q \\ p \leq x}} \log(p) \sim x$$

となるから，

$$\sum_{\substack{p \equiv a \bmod q \\ p \leq x}} \log(p) \sim \frac{x}{\varphi(q)}$$

で，全く同様の式が得られる．そして，この式が本当に正しいかは $\Re(s) = 1$ において $L(s, \chi) \neq 0$ が成り立つかどうかにかかっている．

11.4 ランダウの補題

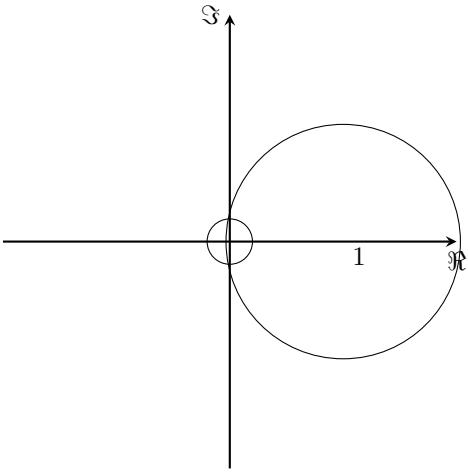
ここで，一旦 $L(s, \chi) \neq 0$ の問題から離れて，ランダウの補題と呼ばれるものを紹介する．

補題 3. $a_n \geq 0$ でディリクレ級数

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

が $\Re(s) > \sigma_0$ で絶対収束するとしよう．そして，$f(s)$ が $\Re(s) \geq \sigma_0$ に特異点を持たずに解析接続できるとする．その時，ある $\varepsilon > 0$ が存在して，ディリクレ級数は $\Re(s) \geq \sigma_0 - \varepsilon$ で収束する．

これを証明していこう．まず，$\sigma_0 = 0$ としても一般性を失わない．そして，解析接続した結果は $s = 0$ において正則なのだから，その近傍は正則である．



よって，$s = 1$ を中心とした，半径 $1+\varepsilon$ の円内と円上も，$\varepsilon > 0$ を十分小さくとることで正則になる．したがって，1 を中心としたテイラー展開が存在する．

$$f(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!}(s-1)^k$$

となる．また，

$$f^{(k)}(s) = \sum_{n=1}^{\infty} \frac{a_n(-1)^k(\log n)^k}{n^s}$$

となるので，

$$f^{(k)}(1) = \sum_{n=1}^{\infty} \frac{a_n(-1)^k(\log n)^k}{n}$$

となり，$(s-1)^k$ を $(1-s)^k$ に変えると，$(-1)^k$ のところが消えて，

$$f(s) = \sum_{k=0}^{\infty} \frac{(1-s)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n(\log n)^k}{n} = \sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{k=0}^{\infty} \frac{(1-s)^k(\log n)^k}{k!}$$

となる．さてここで，e^x のテイラー展開を思い出すと，これは

$$\sum_{n=1}^{\infty} \frac{a_n}{n} n^{1-s}$$

に等しい．ここで，$s = -\varepsilon$ とすれば,

$$\sum_{n=1}^{\infty} a_n n^{\varepsilon} < \infty$$

となる．これは問題のディリクレ級数が $\Re(s) = -\varepsilon$ の時，絶対収束することを示している．したがって，補題は示された.

11.5 L 関数の $\Re(s) = 1$ での非零性

$\Re(s) = 1$ において $L(s, \chi) \neq 0$ を証明していこう．まず

$$f(s) = \prod_{\chi \bmod q} L(s, \chi)$$

について考える．それぞれの L 関数はオイラー積によって表されるから,

$$f(s) = \prod_{p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

ここで，当然

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \exp\left(-\sum_{\chi} \log\left(1 - \frac{\chi(p)}{p^s}\right)\right)$$

であるから，$\log(1 - x)$ のテイラー展開を思い出せば,

$$f(s) = \prod_{\chi \bmod q} L(s, \chi) = \prod_{p} \exp\left(\sum_{\chi} \sum_{n} \frac{\chi(p^n)}{np^{ns}}\right)$$

となる．さてここで,

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi(q) & a \equiv 1 \pmod{q} \\ 0 & otherwise \end{cases}$$

を思い出そう．すると，

$$\prod_p \exp\left(\sum_\chi \sum_n \frac{\chi(p^n)}{np^{ns}}\right) = \prod_p \exp\left(\sum_n \sum_\chi \frac{\chi(p^n)}{np^{ns}}\right)$$
$$= \prod_p \exp\left(\varphi(q) \sum_{p^n \equiv 1 \bmod q} \frac{1}{np^{ns}}\right)$$

となる．そして，これは非負の係数を持つディリクレ級数になっている．したがって $f(s)$ はディリクレ級数である[19]．さてここで，

$$f(s) = \exp(g(s)), g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}, b_n \geq 0$$

とできる．そして，

$$\log |f(\sigma)^3 f(\sigma + it)^4 f(\sigma + 2it)|$$

について考えよう．リーマンゼータ関数の時と同様に

$$\begin{aligned}
&\log |f(\sigma)^3 f(\sigma + it)^4 f(\sigma + 2it)| \\
=&\Re\left(3g(\sigma) + 4g(\sigma + it) + g(\sigma + 2it)\right)) \\
=&\Re\left(3\sum_{n=1}^{\infty} \frac{b_n}{n^\sigma} + 4\sum_{n=1}^{\infty} \frac{b_n}{n^{\sigma+it}} + \sum_{n=1}^{\infty} \frac{b_n}{n^{\sigma+2it}}\right) \\
=&\sum_{n=1}^{\infty} \frac{b_n}{n^\sigma}(3 + 4\cos(t \log n) + \cos(2t \log n)) \\
\geq&0
\end{aligned}$$

となる．よって，

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

[19] $\prod_p$ を exp の中に入れて，$e^z = 1 + z + \frac{z^3}{2!} + \frac{z^3}{3!} + \ldots$ を使う

となる．さてここで，$t \neq 0$ としよう．$L(s, \chi_0)$ は $s = 1$ に一位の極を持つことに留意すると，$f(s)$ も $s = 1$ に一位の極を持つから，両辺を $\sigma - 1$ で割ると，

$$\left|(\sigma-1)^3 f(\sigma)^3 \frac{f(\sigma+it)^4}{(\sigma-1)^4} f(\sigma+2it)\right| \geq \frac{1}{\sigma-1}$$

となる．この時，もし $f(1+it) = 0$ ならば，$\sigma \to 1$ の極限を考えると，左辺は

$$\begin{aligned}&\lim_{\sigma\to 1}\left|(\sigma-1)^3 f(\sigma)^3 \frac{f(\sigma+it)^4}{(\sigma-1)^4} f(\sigma+2it)\right| \\ &= \lim_{\sigma\to 1}\left|R^3 f'(1+it)^4 f(\sigma+2it)\right|\end{aligned}$$

となる．ただし R は $f(s)$ の $s = 1$ の留数である．さてここで，この極限は有限であるが，

$$\lim_{\sigma\to 1}\frac{1}{\sigma-1}$$

は無限大に発散する．これは矛盾である．したがって，$L(s, \chi)$ は $s = 1+it, t \neq 0$ において零点を持たない．しかし，この議論を $t = 0$ に適用することはできない．なぜなら， その時，$f(1+it)$ が極になってしまい，上記の議論が矛盾を生み出さないからである．そこで，$L(1, \chi) \neq 0$ だけ別に証明する．もし，$L(1, \chi) = 0$ だとすると，$s = 1$ において，

$$f(s) = \prod_{\chi} L(s, \chi)$$

は解析的である．なぜならば，$L(s, \chi_0)$ は一位の極を $s = 1$ でもち，それが $L(1, \chi)$ と打ち消し合うからである．よって，$\Re(s) > 0$ で $f(s)$ は解析的である．したがって，ランダウの補題から，$\Re(s) > 0$ において，

$$\prod_p \exp\left(\varphi(q) \sum_{p^n \equiv 1 \bmod q} \frac{1}{np^{ns}}\right) = \exp\left(\sum_p \varphi(q) \sum_{p^n \equiv 1 \bmod q} \frac{1}{np^{ns}}\right)$$

は収束する[20]．したがって $s = 1/\varphi(q)$ においても，これは収束する．さてここで，オイラーの定理

$$p^{\varphi(q)} \equiv 1 \pmod{q}$$

を思い出そう．これから，

$$\sum_{p^n \equiv 1 \bmod q} \frac{1}{np^{ns}}$$

の中には，$n = \varphi(q)$ となる項，すなわち，

$$\frac{1}{\varphi(q)p^{\varphi(q)\frac{1}{\varphi(q)}}} = \frac{1}{\varphi(q)p}$$

が現れるはずである．したがって，$s = 1/\varphi(q)$ において

$$\prod_p \exp\left(\varphi(q) \sum_{p^n \equiv 1 \bmod q} \frac{1}{np^{ns}}\right) \geq \exp\left(\sum_p \frac{1}{p}\right)$$

となるが，素数の逆数和は発散するから，右辺は発散する．しかし，左辺は収束するのであったから，矛盾が生じる．よって，$L(1, \chi) \neq 0$ である．したがって，以上の議論をまとめると，$\Re(s) = 1$ において，$L(s, \chi) \neq 0$ である．よって，

$$\sum_{\substack{p \equiv a \bmod q \\ p \leq x}} \log(p) \sim \frac{x}{\varphi(q)}$$

が成立する．そして，ここから明らかに次の定理が成立する．

定理 6. 初項と公差が互いに素な等差数列には素数が無限に存在する．

これを，ディリクレの算術級数定理という．また，素数定理と $\vartheta(x) \sim x$ などの同値性を示した手順と同様に，次の算術級数の素数定理が成り立つ．

定理 7. 初項 a，公差 d の等差数列に含まれる素数で，x 以下のものの数を $\pi_{d,a}(x)$ とすると，

$$\pi_{d,a}(x) \sim \frac{1}{\varphi(d)} \frac{x}{\log x}$$

となる．

[20] $\Re(s) > u > 0$ までしか収束しないとすると，ランダウの補題から矛盾が起こる．

このように，L 関数やリーマンゼータ関数について，特に，零点や極について考察することで，算術級数定理や素数定理といった，整数に関する結果を得ることができる．このような手法は，解析的整数論において，非常に多く使われる手法である．