

素数定理について

讃岐勝

以下、 p は素数とする。

素数定理

x ($x > 0$) を超えない素数の個数を $\pi(x)$ とおく：

$$\pi(x) = \sum_{p \leq x} 1$$

そのとき、

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1$$

である。

ここで、素数定理

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1$$

を見てみると、 x に近い 2 つの連続した素数間の平均距離はおよそ $\log x$ と考えることができる

素数定理をエラトステネスのふるいを用いて、簡単に誘導してみる。

x までのすべての整数のうちで奇数、2 で割り切れない数は大体 $(1 - \frac{1}{2})$ ある。奇数のうちで、3 で割り切れない数は $\frac{2}{3} (= 1 - \frac{1}{3})$ ある。更に、残っている数のうち、5 で割り切れない数は $1 - \frac{1}{5}$ ある。従って、 x を越えない素数の個数はこれらの積をすべての素数 p にわたって取ればよいので、近似的に

$$\prod_p \left(1 - \frac{1}{p}\right) \cdot x$$

に等しい。更に、 $\prod_p \left(1 - \frac{1}{p}\right)$ は近似的に $\frac{1}{\log x}$ に等しい。

このことを認めると素数定理が導出されたことになる。

ここで、きちんと素数定理の証明を試みる。

[Chebyshev's 関数]

$$\theta(x) = \sum_{p \leq x} \log p, \psi(x) = \sum_{p^m \leq x} \log p \quad (x > 0)$$

であって (但し、 $\theta(y) = 0$ if $y < 2$)

$$\psi(x) = \theta(x) + \theta(x^{\frac{1}{2}}) + \theta(x^{\frac{1}{3}}) + \dots \quad \dots (1)$$

$$\psi(x) = \sum_{p \leq x} \left[\frac{\log x}{\log p} \right] \log p \quad \dots (2)$$

を満たす。

[定理 1]

次の三つの式

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\log x} \right)}, \frac{\theta(x)}{x}, \frac{\psi(x)}{x}$$

は $x \rightarrow \infty$ とするとき、同じ極限を持つ。

[証明]

それぞれの上極限を A_1, A_2, A_3 、下極限を $\lambda_1, \lambda_2, \lambda_3$ とおく。

(1),(2) から

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

よって $A_2 \leq A_3 \leq A_1$

一方、 $0 < \alpha < 1, x > 1$ とすると

$$\theta(x) \geq \sum_{x^\alpha < p \leq x} \log p \geq \{\pi(x) - \pi(x^\alpha)\} \log(x^\alpha)$$

故に、 $\pi(x^\alpha) < x^\alpha$ から

$$\frac{\theta(x)}{x} > \alpha \left(\frac{\pi(x) \log(x)}{x} - \frac{\log x}{x^{1-\alpha}} \right)$$

α を固定して $x \rightarrow \infty$ とすると、

$\log x / x^{1-\alpha} \rightarrow 0$ から、 $A_2 \geq \alpha A_1$ 、よって $A_2 \geq A_1$ 、以上から、 $A_1 = A_2 = A_3$
 λ についても、同様に証明できる。

[定理 2]

x を十分に大きくしたとき、

$$a \frac{x}{\log x} < \pi(x) < A \frac{x}{\log x}$$

を持たすような $a, A > 0$:(constant) が存在する。

[証明]

A, λ を $x \rightarrow \infty$ とした時の上極限、下極限とする。

$$N = \binom{2n}{n} = \frac{(n+1)(n+2)\cdots(2n)}{n!} \text{ を考えると}$$

$(1+1)^{2n}$ の二項定理から

$$N < 2^{2n} < (2n+1)N \quad \cdots (3)$$

今、 N は $n < p \leq 2n$ ある p で割れるので

$$N \geq \prod_{n < p \leq 2n} p$$

これと (3) の式について対数を考えてあげると、

$$2n \log 2 > \log N \geq \sum_{n < p \leq 2n} \log p = \theta(2n) - \theta(n)$$

$n = 2^{r-1}$ とおいて、 $r = 1$ から $r = m$ まで代入して加えると、

$$\theta(x) < \sum_{r=1}^m 2^r \log 2 < 2^{m+1} \log 2$$

故に、 $x > 1$ の時、 $2^{m-1} \leq x < 2^m$ を満たす m を考えると、

$$\theta(x) \leq \theta(2^m) < 2^{m+1} \log 2 \leq 4x \log 2$$

より、 $A \leq 4 \log 2$

今、 $m!$ の p についての指数 $\text{ord}_p m!$ を考えると、1 から m までの p の倍数の個数は $\left[\frac{m}{p} \right]$ であ

り、1 から m までの p^2 の倍数の個数は $\left[\frac{m}{p^2} \right]$ だけある。

従って、1 から m までの p の倍数で、 p^2 の倍数にならないものの個数は

$$\left[\frac{m}{p} \right] - \left[\frac{m}{p^2} \right]$$

である。

同じく、1 から m までの p^2 の倍数で、 p^3 の倍数にならないものの個数は

$$\left[\frac{m}{p^2} \right] - \left[\frac{m}{p^3} \right]$$

である。

同様に、1 から m までの p^k の倍数で、 p^{k+1} の倍数にならないものの個数は

$$\left[\frac{m}{p^k} \right] - \left[\frac{m}{p^{k+1}} \right]$$

である。

$p^l \leq m < p^{l+1}$ のときは、

$$\left[\frac{m}{p^{l+1}} \right] = 0$$

であり、 $l+1 \leq j$ については、

$$\left[\frac{m}{p^j} \right] = 0$$

よって、 $m!$ に含まれる p の指数 $\text{ord}_p m!$ は

$$\begin{aligned} \text{ord}_p m! &= 1 \left(\left[\frac{m}{p} \right] - \left[\frac{m}{p^2} \right] \right) + 2 \left(\left[\frac{m}{p^2} \right] - \left[\frac{m}{p^3} \right] \right) + \cdots + l \left(\left[\frac{m}{p^l} \right] - \left[\frac{m}{p^{l+1}} \right] \right) \\ &= \left[\frac{m}{p} \right] + \left[\frac{m}{p^2} \right] + \cdots + \left[\frac{m}{p^l} \right] + 0 + \cdots \\ &= \sum_{k=1}^{\infty} \left[\frac{m}{p^k} \right] \end{aligned}$$

となる。

これを用いて、 $N = \frac{(2n)!}{(n!)^2}$ の p に対する指数 $\text{ord}_p N = \frac{(2n)!}{(n!)^2} = v_p$ は

$$v_p = \left[\frac{2n}{p} \right] + \left[\frac{2n}{p^2} \right] + \cdots - 2 \left(\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \cdots \right)$$

となり、 $p^{M_p} \leq 2n \leq p^{M_p+1}$ となる $M_p = \left\lceil \frac{\log 2n}{\log p} \right\rceil$ を考えると、

$$v_p = \sum_{r=1}^{M_p} \left(\left[\frac{2n}{p^r} \right] - 2 \left[\frac{n}{p^r} \right] \right) \leq M_p$$

となり、 $[2y] - 2[y] = 0$ or 1 であり (2) から

$$e^{\psi(2n)} = \prod_{p \leq 2n} p^{M_p}$$

となる。よって、 $e^{\psi(2n)}$ は N で割れて、(3) から

$$2n \log 2 - \log(2n+1) < \log N \leq \psi(2n)$$

故に $x > 2$, $n = \lfloor \frac{1}{2}x \rfloor$ とすると

$$\psi(x) \geq \psi(2n) > (x-2) \log 2 - \log(x+1)$$

より、 $\lambda \geq \log 2$
 $\log 2 \leq \lambda \leq \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} \leq A \leq 4 \log 2$ となり定理を満たす

[ゼータ関数]

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

をゼータ関数という。

また、 $\text{Res} > 1$ で、

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} \quad (p: \text{素数}) \quad \dots (4)$$

と無限積に展開される。

$\sum_{s=1}^{\infty} \frac{1}{1-p^{-s}}$ ($s > 1$) について、対数をとると

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}$$

この両辺を s で微分すると

$$\frac{\zeta'(s)}{\zeta(s)} = - \sum_p \sum_{m=1}^{\infty} \frac{\log p}{mp^{ms}} = - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

ここで、

$$\Lambda(n) = \begin{cases} 2 \log p & n = p^m \quad (m = 1, 2, \dots) \\ 0 & \text{その他の場合} \end{cases}$$

であり、Chebyshev 関数より

[定理]

$$\liminf_{x \rightarrow \infty} \pi(x) / \frac{x}{\log x} \leq 1 \leq \limsup_{x \rightarrow \infty} \pi(x) / \frac{x}{\log x}$$

[証明]

$$f(s) = - \frac{\zeta'(s)}{\zeta(s)} \text{ として}$$

$$\begin{cases} \liminf_{x \rightarrow \infty} \frac{\psi(x)}{x} = A \\ \limsup_{x \rightarrow \infty} \frac{\psi(x)}{x} = \lambda \end{cases}$$

$$\begin{cases} \liminf_{x \rightarrow \infty} (s-1)f(s) = A' \\ \limsup_{x \rightarrow \infty} (s-1)f(s) = \lambda' \end{cases}$$

$\Lambda \neq \infty$ でないとき、 $B > \Lambda$ なる B が選べる。
 $\frac{\psi(x)}{x} < B$ for all $x \geq x_0 = x_0(B), x_0 > 1$

$s > 1$ について

$$\begin{aligned} f(s) &= s \int_1^\infty \frac{\psi(x)}{x^{s+1}} dx < s \int_1^{x_0} \frac{\psi(x)}{x^{s+1}} dx + s \int_{x_0}^\infty \frac{B}{x^s} dx \\ &= s \int_1^{x_0} \frac{\psi(x) - Bx}{x^{s+1}} dx + \frac{sB}{s-1} \\ &\leq s \int_1^{x_0} \frac{|\psi(x) - Bx|}{x^2} dx + \frac{sB}{s-1} \end{aligned}$$

よって、 $(s-1)f(s) \leq s(s-1)K + sB$ 但し、 $K = K(B, x_0) = K(B)$
 $s \rightarrow 1+0$ とすると、 $\Lambda' \leq B, B > \Lambda$ より $\Lambda' \leq \Lambda$ となる。
 似たようにして $\lambda' \geq \lambda$ を導くことができる。故に

$$\lambda \leq \lambda' \leq \Lambda' \leq \Lambda$$

今、 x^{-s} は減少関数で s を固定してやると

$$\begin{aligned} \int_1^\infty \frac{dx}{x^s} &< \sum_{n=1}^\infty \frac{1}{n^s} < 1 + \int_1^\infty \frac{dx}{x^s} \\ \text{i.e.} \quad \frac{1}{s-1} &< \zeta(s) < \frac{s}{s-1} \end{aligned}$$

故に、 $(s-1)\zeta(s) \rightarrow 1$ as $s \rightarrow 1+0$

$\frac{\log x}{x^s}$ ($x \geq e, s > 1$) は減少関数であるので、 $s \rightarrow 1+0$ を考えると

$$\begin{aligned} -\zeta'(s) &= \sum_{n=1}^\infty \frac{\log n}{n^s} = \int_1^\infty \frac{\log x}{x^s} dx + O(1) \\ &= \frac{1}{(s-1)^2} \int_0^\infty ye^{-y} dy + O(1) \quad (x^{s-1} = e^y) \\ &= \frac{1}{(s-1)^2} + O(1) \end{aligned}$$

故に

$$(s-1)f(s) = \frac{-(s-1)^2 \zeta'(s)}{(s-1)\zeta(s)} \rightarrow 1 \quad \text{as } s \rightarrow 1+0$$

なので、 $\Lambda' = \lambda' = 1$

これより、素数定理が示すことができた

さらに、素数定理をうまく近似してやる。素数の密度関数は $\frac{\pi(x)}{x}$ なので

$$\frac{\pi(x)}{x} \sim \frac{1}{\log x} \quad (x \rightarrow \infty)$$

であり、 $\frac{1}{\log x}$ が 1 から x までの平均的な素数の密度と考えられ、これを x の近くの素数の密度と考えて、区間 $[1, x]$ を小区間に区切って積分してみる。

$$Li(x) = \int_2^x \frac{dt}{\log t}$$

$Li(x)$ は積分対数関数と呼ばれ、 $\pi(x)$ を $\frac{1}{\log x}$ で近似するより、対数積分を用いた $Li(x)$ の近似は更に適切な素数分布の近似式になっている。

今まで述べてきた素数と言うのは無限に存在している。今、無限性を (4) の式を用いて証明する

[素数の無限性の証明]

今、素数が有限個しか存在しないとす。調和関数

$$\sum_{n=1}^{\infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots$$

は無限大に発散する。またこの式は

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_p \frac{1}{1 - \frac{1}{p}}$$

と書けるので

$$\prod_p \frac{1}{1 - \frac{1}{p}} \sim \infty$$

また、 $\log \prod_p (1 - \frac{1}{p}) = \sum_p \log(1 - \frac{1}{p})$ 。

$\frac{1}{p} < 1$ から、マクローリン展開より

$$\sum_p \log(1 - \frac{1}{p}) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^m} = \sum_p \frac{1}{p} + \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^m}$$

今、

$$\sum_{m=2}^{\infty} \frac{1}{mp^m} < \sum_{m=2}^{\infty} \frac{1}{p^m} = \frac{1}{p(1 - \frac{1}{p})} \leq \frac{2}{p^2}$$

従って

$$\log \prod_p (1 - \frac{1}{p}) < \sum_p \frac{1}{p} + 2(\sum_p \frac{1}{p^2})$$

$\sum_n \frac{1}{n^2}$ は収束するので、 $\sum_p \frac{1}{p^2}$ も収束する。

$\sum_p \frac{1}{p}$ が収束すると仮定すると、

$$\exists M : (\text{constant}) \text{ s.t. } \log \prod_p \left(1 - \frac{1}{p}\right) < M \text{ or } \prod_p \left(1 - \frac{1}{p}\right) < e^M$$

しかしながら、 $\prod_p \left(1 - \frac{1}{p}\right) \rightarrow \infty$ as $n \rightarrow \infty$ なので矛盾が生じる。よって $\sum_p \frac{1}{p}$ は発散する。

$\sum_p \frac{1}{p}$ は発散して、その調和関数 $\sum_p p$ はもちろん発散する。よって、素数は無限に存在することが示せた。

入学後に研究したい分野

昔からも興味を持っていた素数というものを大学に入っているいろいろな講義を受ける中で、もっと詳しく学びたいと思うようになりました。素数でイデアルを考えるとそれで生成された剰余環は整域である、中国剰余定理についての代数的証明・環論での証明など多方面の分野に行き渡る証明がまったく違うようで実は共通点があったり、解析的なもので見ると、ゼータ関数や級数の和や素数定理など素数などを何らかの関係式にして表すことや、コンピュータによる解析など様々な形で論文・研究がされていて、より深く学んでみたいと思いました。日常、目にする整数・素数についてもっと学んでみたいと思います。大学院入学後は、素数を中心とした数論というものを研究していきたいと思っています。