算術級数定理のお話 … L函数入門

平成27年夏から秋にかけて
富山県教育委員会小中学校課
児童生徒育成係　主幹
片山　喜美

「算術級数定理」というのは、**「初項 a と公比 d が互いに素である算術級数（等差数列）の中に、素数が無数に含まれている。」**というものである。

この定理によれば、例えば、「一の位の数が1である数 1,11,21,31,41,51,61,.....　の中に無限個の素数がある」ということが言える。なぜなら、算術級数定理で初項1、公差10の場合であるからである。

素数が無数に存在することの証明は、はるか昔 (紀元前3世紀頃？)、ユークリッド（古代ギリシャの数学者・天文学者）により与えられていた。その証明は極めてシンプルである。素数が有限個であると仮定し、それらすべてを掛け合わせたものに1を加えた数の素因数を考え、矛盾を導くという背理法を用いるのである。

算術級数定理も背理法で、シンプルな証明を与えられるのかというと、実はそう簡単にいかない。この定理に関するDirichletによる証明は、ある種の複素関数の微分や特異点、零点などの性質を駆使するものである。定理の述べている内容からは、どうしてそういったものを用いるのか不思議な感じがする。証明には長い道のりが必要であるが、まず具体的な場合について、少し考察してみる。

1　素数に関する基本的な事項

1.1　素数は無限にある

自然数をなるべく小さい自然数の積に分解することを考える。

- 2,3はそれより小さな数（1を除く）で割り切れない。そういった数を素数 (prime number) という。

定義　$p \in \mathbb{N}$ が素数である　$\Longleftrightarrow$　p の約数がちょうど2つある
＜注意＞1は素数に含めない。

- $4 = 2 \times 2 = 2^2$ と因数分解できる。こうした数を合成数という。
- 5は素数、　$6 = 2 \times 3$、　7は素数、　$8 = 2^3$,　$9 = 3^2$,　$10 = 2 \times 5$

定理１．１（ユークリッド）　素数は無限にある。

証明）背理法による。素数が有限個しかないと仮定し、それらが $p_1, p_2, \cdots p_k$ で全てであるとする。このとき、$N = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$ とおく。すると、N はどの素数 $p_1, p_2, \cdots, p_k$ で割っても1余る。従って、N が新たな素数であるか、例え合成数であってもその素因数は $p_1, p_2, \cdots, p_k$ とは異なる。これは、素数が $p_1, p_2, \cdots, p_k$ だけであるという仮定に矛

盾する。//

＜注意＞　素数を $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \cdots$ と小さい順に並べていき、上の証明の N を考える。
$p_1+1 = 3$,　$p_1p_2+1 = 7$,　$p_1p_2p_3+1 = 31$,　$p_1p_2p_3p_4+1 = 211$,　$p_1p_2p_3p_4p_4+1 = 2311$
これらはすべて素数である。しかし,
$p_1p_2p_3p_4p_5p_6 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$ と合成数となる。

$p_1p_2 \cdots p_k + 1$ については、この後もしばらく合成数が続いて、素数が出てこない。もう素数は出てこないのか？

定理 1．1 の別証）素数が有限個しかないと仮定し、その最大のものを p とする。
このとき、 $p! + 1$ は p 以下のどんな数でも割り切れないので、 p を超える素数がなければならない。これは矛盾。//

＜注意＞　$n! + 1$ を順に考えて、素数かどうかを調べていると、どういう状況になるのだろうか。

1.2　素数の判定（最も単純な方法）

ある数が素数であるかどうかを調べるには、その数を小さい数で順に割っていくのが一番単純な方法である。例えば、73 が素数かづか調べるには、2 で割って余り 1、3 で割って余り 1、5 で割って余り 3、7 で割って余り 3、11 で割って余り 7、...
書くのが面倒になってくるので、記号を導入する。「n を N で割った余りが r である」ことを「 $n \equiv r \pmod N$」と書くことにする。すると
$73 \equiv 1 \pmod 2$,　$73 \equiv 1 \pmod 3$,　$73 \equiv 3 \pmod 5$,　$73 \equiv 3 \pmod 7$,
$73 \equiv 7 \pmod{11}$,　$73 \equiv 8 \pmod{13}$,　$\cdots$
このあと順に続けていっても余りが 0（すなわち割り切れる）となることがない。その結果、73 は素数であることがわかる。

ところで、上の作業は $\pmod 7$ までで終えてよい。なぜなら $73 = a \times b$ と積に表わされ、 $a \leq b$ とすると、$73 = ab \geq a^2$。従って、 $a \leqq \sqrt{73}$。すなわち、もし合成数なら、$\sqrt{73}$ より小さな素因数を持つことになるのである。$\sqrt{73} < 9$ なので、7 まで調べて割り切れなければ素数であるといってよい。

命題 1．1　　n が合成数なら、n は $\sqrt{n}$ 以下の素因数を持つ。
従って、$\sqrt{n}$ 以下の素数で割ってみて割り切れなかったら素数だと判定できる。

例.　　$\sqrt{89} < 10$
$89 \equiv 1 \pmod 2$,　$89 \equiv 2 \pmod 3$,　$89 \equiv 4 \pmod 5$,　$89 \equiv 5 \pmod 7$
よって 89 は素数である。

1.3　素数のリスト作り … 篩の方法

素数を小さい順に並べていくことを考える。きりがないので、300 未満の素数とする。先の方法で $\sqrt{n}$ 以下の素数で割って、 n が素数かどうかを $n \leq 300$ についてそれぞれ考えて行けばいいのだが、相当な時間がかかる。(コンピュータ・プログラムを作成すればいいかもしれない。)

300 未満と区切るのならば、合成数を消去していく方法が速い。次のような作業をする。

- 2 から 299 までの数をリストする。
- 2 は素数。その倍数 $4, 6, 8, \cdots, 296, 298$ は合成数だから消去する。
- リストで消去されていない数で最も小さい 3 は素数である。その倍数で消えていない $9, 15, 21, \cdots, 291, 297$ を消去する。
- リスト消去されていない数で最も小さい 5 は素数である。その倍数で消えていないものをリストから消去する。

以下、同様の作業を続けて行けば、合成数がふるい落とされ、素数だけが残る。
実際には、一ケタの素数,2,3,5,7 のあと、10 以上は偶数や一の位が 5 の数ははじめから除外したリストから篩にかけていけばよい。

2	3	5	7	101	103	107	109	~~201~~	~~203~~	~~207~~	~~209~~
11	13	17	19	~~111~~	113	~~117~~	~~119~~	211	~~213~~	~~217~~	~~219~~
~~21~~	23	~~27~~	29	~~121~~	~~123~~	127	~~129~~	~~221~~	223	227	229
31	~~33~~	37	~~39~~	131	~~133~~	137	139	~~231~~	233	~~237~~	239
41	43	47	~~49~~	~~141~~	~~143~~	~~147~~	149	241	~~243~~	~~247~~	~~249~~
~~51~~	53	~~57~~	59	151	~~153~~	157	~~159~~	251	~~253~~	257	~~259~~
61	~~63~~	67	~~69~~	~~161~~	163	167	~~169~~	~~261~~	263	~~267~~	269
71	73	~~77~~	79	~~171~~	173	~~177~~	179	271	~~273~~	277	~~279~~
~~81~~	83	~~87~~	89	181	~~183~~	~~187~~	~~189~~	281	283	~~287~~	~~289~~
~~91~~	~~93~~	97	~~99~~	191	193	197	199	~~291~~	293	~~297~~	~~299~~

上のリストで二重線で消したものが合成数で、残ったものが素数である。手書きで 15 分程度で作業を終えられるのではないだろうか。このような方法を**「エラトステネスの篩の方法」**という。

課題　エラトステネスの篩の方法で 1000 未満の素数のリストを作るプログラムを作成せよ。

1.4　N で割った余りによる素数の整理

- 2 以外の素数はすべて奇数 (odd number) である。
  ※ 2 を the oddest number と呼ぶらしい。
- 3 で割った余りで整理する。(3 を除く)

余り 1	7	13	19	31	37	43	61	67	73	79	97	103	109	127	139	$\cdots$
余り 2	2	5	11	17	23	29	41	47	53	59	71	83	89	101	107	$\cdots$

- 4 で割った余りで整理する。(2 を除く)

余り 1	5	13	17	29	37	41	53	61	73	89	97	101	109	113	$\cdots$
余り 3	3	7	11	19	23	31	43	47	59	67	71	79	83	103	$\cdots$

- 5 で割った余りで整理する。(5 を除く)

余り 1	11	31	41	61	71	101	131	151	181	191	$\cdots$			
余り 2	2	7	17	37	47	67	7	107	127	137	157	167	197	$\cdots$
余り 3	3	13	23	43	53	73	83	103	113	163	173	193	$\cdots$	
余り 4	19	29	59	79	89	109	139	149	199	$\cdots$				

- 6 で割った余りで整理する。(2,3 を除く)

余り 1	7	13	19	31	37	43	61	67	73	79	97	103	109	127	139	$\cdots$
余り 5	5	11	17	23	29	41	47	53	59	71	83	89	101	107	113	$\cdots$

- 7 で割った余りで整理する。(7 を除く)

余り 1	29	43	71	113	127	197	211	239	281	$\cdots$		
余り 2	2	23	37	79	107	149	163	191	233	$\cdots$		
余り 3	3	17	31	59	73	101	157	199	227	241	269	$\cdots$
余り 4	11	53	67	109	137	151	193	263	277	$\cdots$		
余り 5	5	19	47	61	89	103	131	173	229	257	271	$\cdots$
余り 6	13	41	83	97	139	167	181	223	251	293	$\cdots$	

ここまで調べた結果から、**「自然数 N と r が互いに素であるとき、N で割った余りが r の素数は無限個ある」**ということは正しそうである。

そのうちのいくつかは、素数が無限個あることに関するユークリッドの証明と同様の方法で証明することができる。

補題１．１　a, b　ともに 4 で割って 1 余る数である時、その積 ab もまた 4 で割って 1 余る数である。

証明)　$a = 4k + 1, b = 4l + 1$ とおいて、$ab = (4k + 1)(4l + 1) = 4(4kl + k + l) + 1$ //

定理１．２　4 で割って 3 余る素数は無限にある。

証明）4 で割って 3 余る素数が $p_1, p_2, \cdots p_k$ で全てであるとする。$N = 4p_1p_2 \cdots p_k - 1$ とおくと、N は 4 で割って 3 余る数である。そして、N は $p_1, p_2, \cdots, p_k$ のいずれでも割り

切れない。従って、N は、 $p_1, p_2, \cdots, p_k$ 以外の素因数を持つ。

もし、N の素因数がすべて 4 で割って 1 余るものであるとすると、補題 1 により、その積は 4 で割って 1 余るから、 N は 4 で割って 1 余ることになる。そのため、N の素因数の中には少なくても 1 つ 4 で割って 3 余るものが含まれていなければならない。これは、仮定に矛盾する。//

課題 6 で割って 5 余る素数が無限個あることを定理 2 と同様の方法で証明せよ

次に、4 で割って 1 余る素数について考える。次の補題が必要である。

補題１．２　p を素数とする。
$a^2 + 1 \equiv 0 \pmod{p}$ を満たす a が存在する。$\Longleftrightarrow$　$p \equiv 1 \pmod{4}$
証明は、ここでは省略する。

定理１．３　4 で割って 1 余る素数は無限にある。
証明） 4 で割って 1 余る素数が $p_1, p_2, \cdots p_k$ で全てであるとする。$N = 4p_1^2 p_2^2 \cdots p_k^2 + 1$ とおくと、N は 4 で割って 1 余る数である。そして、N は $p_1, p_2, \cdots, p_k$ のいずれでも割り切れない。従って、N は、 $p_1, p_2, \cdots, p_k$ 以外の素因数を持つ。

N の素因数の 1 つを p とすると、 $N \equiv 0 \pmod{p}$ より、 $(2p_1 p_2 \ldots p_k)^2 + 1 \equiv 0 \pmod{p}$ 。補題 2 より、こうなるのは $p \equiv 1 \pmod{4}$ のときである。これは、4 で割って 1 余る素数が $p_1, p_2, \cdots p_k$ で全てであることに矛盾する。//

さて、3 で割って余り 1 、2 の素数についてはどうなのか？

この場合、4 で割って余り 1 、3 の時のような背理法では証明ができない。無限級数で作る解析関数を用いて証明していくことになる。そのため、次節では、無限級数について少し調べていく。

2　調和級数の発散と素数が無限個あることについての別証明

2.1　調和級数の発散

命題２．１　$\displaystyle\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$

証明）$\displaystyle S_N = \sum_{n=1}^{N} \frac{1}{n}$ とおく。 $S_1 < S_2 < \cdots < S_N < \cdots$ と単調増加となる。

$$
\begin{aligned}
S_{2^m} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^{m-1}+1} + \cdots + \frac{1}{2^m}\right) \\
&> 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^m} + \cdots + \frac{1}{2^m}\right) \\
&= 1 + \frac{1}{2} + 2 \times \frac{1}{4} + 4 \times \frac{1}{8} + \cdots + 2^{m-1} \times \frac{1}{2^m} \\
&= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2} = 1 + \frac{1}{2}m
\end{aligned}
$$

従って、$\displaystyle\lim_{m\to\infty} S_{2^m} \geqq \lim_{m\to\infty} \left(1 + \frac{m}{2}\right) = +\infty$　//

別証）$k<x<k+1 \quad (k\in\mathbb{N})$ のとき、$\dfrac{1}{k}>\dfrac{1}{x}>\dfrac{1}{k+1}$ より、

$$\int_k^{k+1}\frac{1}{k}dx>\int_k^{k+1}\frac{1}{x}dx>\int_k^{k+1}\frac{1}{k+1}dx$$

$$\frac{1}{k}>[\log x]_k^{k+1}=\log(k+1)-\log k$$

$$S_N=\sum_{k=1}^{N}\frac{1}{k}>\sum_{k=1}^{N}\{\log(k+1)-\log k\}=\log(N+1)$$

よって、$\lim\limits_{N\to\infty}S_N\geqq\lim\limits_{N\to\infty}\log(N+1)=+\infty \quad //$

2.2　素数が無限個あることの別証明

命題２．２　$\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^s}$ は $s>1$ のとき絶対収束する。これを $\zeta(s)$ と書く。

証明は、ここでは省略する。

命題２．３　$s>1$ のとき、

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p:\text{素数}}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}+\cdots\cdots\right)=\prod_{p:\text{素数}}\left(\frac{1}{1-\dfrac{1}{p^s}}\right)$$

これも証明は、省略する。

命題２．４　$|x|<1$ のとき、$\log(1-x)^{-1}=\displaystyle\sum_{r=1}^{\infty}\frac{x^r}{r}$

証明）$|x|<1$ のとき、$1+x+x^2+\cdots+x^{n-1}+\cdots=\dfrac{1}{1-x}$

これは絶対収束であるから、両辺を積分するとき、左辺を項別に積分できる。よって、

$x+\dfrac{x^2}{2}+\cdots+\dfrac{x^n}{n}+\cdots=-\log(1-x)$ //

命題２．５　$\log\zeta(s)=\displaystyle\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}$

証明）$\log\zeta(s)=\log\displaystyle\prod_{p:\text{素数}}\left(1-p^{-s}\right)^{-1}=\sum_{p:\text{素数}}\log\left(1-p^{-s}\right)^{-1}=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\frac{(p^{-s})^r}{r}$

$$=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}} \qquad //$$

定理２．１　$\displaystyle\sum_{p:\text{素数}}\frac{1}{p}=+\infty$

証明）$\lim\limits_{s\to1+0}\zeta(s)=\displaystyle\sum_{n=1}^{\infty}\frac{1}{n}=+\infty$　より　$\lim\limits_{s\to1+0}\log\zeta(s)=+\infty$

従って、命題２．５より　$\lim_{s\to 1+0}\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}=+\infty$

ここで、和を r $=1$ と $r\geqq 2$ の２つの部分に分けて、

$$\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}=\sum_{p:素数}\frac{1}{p^s}+\sum_{p:素数}\sum_{r=2}^{\infty}\frac{1}{rp^{rs}}$$

この第２の和で $s=1$ として、

$$A=\sum_{p:素数}\sum_{r=2}^{\infty}\frac{1}{rp^{r}}\quad<\sum_{p:素数}\sum_{r=2}^{\infty}\frac{1}{2p^{r}}=\sum_{p:素数}\frac{1}{2}\frac{\frac{1}{p^2}}{1-\frac{1}{p}}=\sum_{p:素数}\frac{1}{2}\frac{1}{p(p-1)}<\frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{n(n-1)}$$

ここで、$\sum_{n=2}^{N}\frac{1}{n(n-1)}=\sum_{n=2}^{N}\left(\frac{1}{n-1}-\frac{1}{n}\right)=1-\frac{1}{N}\to 1\quad(N\to\infty)$

よって、$0<A<\frac{1}{2}$。すなわち、２つに分けた和のうち $r\geqq 2$ の部分は $s\to 1+0$ の時に有限である。

全体としては発散するのであるから、$\lim_{s\to 1+0}\sum_{p:素数}\frac{1}{p^s}=+\infty$//

系　素数は無限個ある。

証明）もし、素数が有限個しかないならば、$\sum_{p:素数}\frac{1}{p}$ は有限和であるから収束する。それは定理２．１に矛盾する。従って、素数は無限個ある。//

素数が無限個あることについては、ユークリッドの証明方法がシンプルであり、上の方法は複雑である。しかし、類似の方法を用いてもっといろいろなことを証明していけるのである。

例えば、素数のうち、3で割って1余るものが無限個あることを示すには、$\sum_{\substack{p:素数\\ 3\text{で割って}1\text{余る}}}\frac{1}{p}=+\infty$

を示せばよい。

3　算術級数定理　3で割って1余る素数の場合の証明の考察

3.1　ある種の無限級数と和の分割

次の和 S を考えてみる。

$$S=\sum_{\substack{p:素数\\ p^r\equiv 1\pmod 3}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}$$

(I) 和 S を $r=1$ と $r\geqq 2$ の２つに分ける。

$$S=\sum_{\substack{p:素数\\ p\equiv 1\pmod 3}}\frac{1}{p^s}+\sum_{\substack{p:素数\\ p^r\equiv 1\pmod 3}}\sum_{r=2}^{\infty}\frac{1}{rp^{rs}}$$

(1) 第1の和は、$s \to 1+0$ としてときに「3で割って1余る素数の逆数の和」となるのである。

(2) 第2の和は、$s=1$ とすると、定理2の証明で $A = \sum_{p:素数} \sum_{r=2}^{\infty} \frac{1}{rp^r}$ とおいて考えたものの部分和である。（素数のうち、$p^r \equiv 1 \pmod 3$ となるもののみの和である。）正の数の和であり、$0 < A < \frac{1}{2}$ であったことから、$\sum_{\substack{p:素数 \\ p^r \equiv 1 \pmod 3}} \sum_{r=2}^{\infty} \frac{1}{rp^r}$ は有限な値に収束する。

従って、もし $\lim_{s \to 1+0} S = +\infty$ を示すことができたらならば、第1の和が正の無限大に発散することが結論できる。

(II) S を $\log \zeta(s)$ に類似の関数に結び付けて $\lim_{s \to 1+0} S = +\infty$ を示す。

＜ $n \equiv 1 \pmod 3$ となる n だけ取り出す関数＞

S の2重和は「$p^r \equiv 1 \pmod 3$ を満たす素数 p と r の組み合わせ」に限定されている。そのような組み合わせだけ取り出すために、次のような関数があると都合がよい。

$$Fil(n) = \begin{cases} 1 & (n \equiv 1 \pmod 3) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

※条件を満たす時だけ取り出す"filter"の意味で Fil という関数にしてみた。

すると、$S = \sum_{p:素数} \sum_{r=1}^{\infty} Fil(p^r) \frac{1}{rp^{rs}}$ とできる。p が素数全体にわたるような和にするが、関数 Fil により、条件を満たすものだけ生き残ることになるのである。さて、関数 Fil をどうやって作るか？

天下り的であるが、

$$\chi(n) = \begin{cases} 0 & (n \equiv 0 \pmod 3) \\ 1 & (n \equiv 1 \pmod 3) \\ -1 & (n \equiv 2 \pmod 3) \end{cases}$$

という関数を用いて考えていく。（「指標（character）」と呼ばれる関数である。）

補題３．１ $\chi(ab) = \chi(a)\chi(b) \quad \text{for } {}^{\forall}a, b \in \mathbb{Z}$

証明) a, b がそれぞれ $0, 1, 2 \pmod 3$ のときの9通りについて考えればよい。

(1) $a \equiv 0$ もしくは、$b \equiv 0$ のとき（5通りある）

・ $ab \equiv 0$ なので、$\chi(ab) = 0$

・ $\chi(a)=0$ もしくは、 $\chi(b)=0$ であるから、 $\chi(a)\chi(b)=0$
よって、 $\chi(ab)=\chi(a)\chi(b)$

(2) $(a,b)=(1,1),\,(2,2)$ のとき
・$ab\equiv 1$ なので、 $\chi(ab)=1$
・$(\chi(a),\chi(b))=(1,1),\,(-1,-1)$ であるから、 $\chi(a)\chi(b)=1\cdot 1=(-1)\cdot(-1)=1$
よって、 $\chi(ab)=\chi(a)\chi(b)$

(3) $(a,b)=(1,2),\,(2,1)$ のとき
・$ab\equiv 2$ なので、 $\chi(ab)=-1$
・$(\chi(a),\chi(b))=(1,-1),\,(-1,1)$ であるから、$\chi(a)\chi(b)=1\cdot(-1)=(-1)\cdot 1=-1$
よって、 $\chi(ab)=\chi(a)\chi(b)$

以上から、すべての組み合わせで補題 1 の主張が正しい。//

$$\chi_0(n)=\begin{cases}0 & (n\equiv 0\ (\mathrm{mod}\ 3)\,)\\ 1 & (\text{それ以外のとき})\end{cases}$$

という関数も考える。そして、 $Fil(n)=\dfrac{1}{2}\{\chi_0(n)+\chi(n)\}$ とおく。

補題３．２　　$$Fil(n)=\begin{cases}1 & (n\equiv 1\ (\mathrm{mod}\ 3)\,)\\ 0 & (\text{それ以外のとき})\end{cases}$$

証明）

- $Fil(0)=\dfrac{1}{2}(0+0)=0$
- $Fil(1)=\dfrac{1}{2}(1+1)=1$
- $Fil(2)=\dfrac{1}{2}\{1+(-1)\}=0$　//

＜ S の発散＞

$$S=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}Fil(p^r)\frac{1}{rp^{rs}}=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\frac{1}{2}\left\{\chi_0(p^r)+\chi(p^r)\right\}\frac{1}{rp^{rs}}$$
$$=\frac{1}{2}\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\chi_0(p^r)\frac{1}{rp^{rs}}+\frac{1}{2}\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\chi(p^r)\frac{1}{rp^{rs}}=\frac{1}{2}C+\frac{1}{2}D$$

$$C=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\chi_0(p^r)\frac{1}{rp^{rs}}=\sum_{\substack{p:\text{素数}\\ p\neq 3}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}$$
$$=\sum_{p:\text{素数}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}-\sum_{r=1}^{\infty}\frac{1}{r\cdot 3^{rs}}=\log\zeta(s)-\log(1-3^{-s})^{-1}$$

従って、$s\to 1+0$ のとき $C\to+\infty$

$$D=\sum_{p:素数}\sum_{r=1}^{\infty}\chi(p^r)\frac{1}{rp^{rs}}=\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{r}\left(\frac{\chi(p)}{p^s}\right)^r=\sum_{p:素数}\log\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$
$$=\log\prod_{p:素数}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

ここで、次の補題を使う。

補題３．３　$\displaystyle\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_{p:素数}\frac{1}{1-\dfrac{\chi(p)}{p^s}}$

証明は一旦後回しにする。

先の式に補題３を当てはめると、$D=\log\displaystyle\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$

ここで、$s=1$ とし、さらに、$n=3k,3k+1,3k+2$ に和を分けて考えると、

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n}=\sum_{k=1}^{\infty}\frac{\chi(3k)}{3k}+\sum_{k=0}^{\infty}\frac{\chi(3k+1)}{3k+1}+\sum_{k=0}^{\infty}\frac{\chi(3k+2)}{3k+2}=0+\sum_{k=0}^{\infty}\frac{1}{3k+1}+\sum_{k=0}^{\infty}\frac{-1}{3k+2}$$
$$=\sum_{k=0}^{\infty}\frac{1}{(3k+1)(3k+2)}<\sum_{k=0}^{\infty}\frac{1}{(3k)\cdot(3k)}=\frac{1}{9}\cdot\zeta(2)<+\infty$$

従って、$0<\displaystyle\sum_{n=1}^{\infty}\frac{\chi(n)}{n}<\frac{1}{9}\cdot\zeta(2)$ となり、$s\to1+0$ のとき D は有限。

従って、$s\to1+0$ のとき $S\to+\infty$

(I)、(II) の結果から、$\displaystyle\sum_{\substack{p:素数\\ p\equiv1\pmod 3}}\frac{1}{p}=+\infty$

これにより、次の定理を得る。

定理３．１　３で割った余りが１である素数は無限個ある。

証明）もし有限個しかなかったとしたら、上記の和は有限和であり、$+\infty$ となることはない。//

では、余りが２の場合はどうか？

定理３．２　３で割った余りが２である素数は無限個ある。

証明）定理３の証明で用いた「$n\equiv1\pmod 3$ のときだけ生き残る関数　$Fil(n)$」を「$n\equiv2\pmod 3$ のときだけ生き残る関数　$Fil(n)$」に取り換えればよい。
それには、$Fil(n)=\dfrac{1}{2}\{\chi_0(n)-\chi(n)\}$ とすればうまくいく。（証明は簡単）

前と同様に、$S=\sum_{\substack{p:素数\\ p^r\equiv 2 \pmod 3}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}$　とおく。

(I) $S=\sum_{\substack{p:素数\\ p\equiv 2 \pmod 3}}\frac{1}{p^s}+\sum_{\substack{p:素数\\ p^r\equiv 2 \pmod 3}}\sum_{r=2}^{\infty}\frac{1}{rp^{rs}}$

であり、第2の和は、有限である。(前と同様)

(II) $S=\sum_{p:素数}\sum_{r=1}^{\infty}Fil(p^r)\frac{1}{rp^{rs}}=\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{2}\left\{\chi_0(p^r)-\chi(p^r)\right\}\frac{1}{rp^{rs}}$

$=\frac{1}{2}\sum_{p:素数}\sum_{r=1}^{\infty}\chi_0(p^r)\frac{1}{rp^{rs}}-\frac{1}{2}\sum_{p:素数}\sum_{r=1}^{\infty}\chi(p^r)\frac{1}{rp^{rs}}=\frac{1}{2}C-\frac{1}{2}D$

C,D は前と同じで、$\lim_{s\to 1+0}C=+\infty$,　$\lim_{s\to 1+0}D$ は有限

従って、$s\to 1+0$ のとき $S\to+\infty$

(I)、(II) の結果から、$\sum_{\substack{p:素数\\ p\equiv 2 \pmod 3}}\frac{1}{p}=+\infty$

これにより、3で割った余りが2である素数は無限個あることが帰結される。//

4　算術級数定理　4で割った余りの時や5で割った余りの時の考察

4.1　4で割った余りのとき

定理４．１　4で割って余りが1である素数、4で割って余りが3である素数は無限個ある。

証明)3で割った余りが1、3で割った余りが2である素数の時と同様な方法で示すことができる。

(I) のところは、全く同じである。

(II) で問題となるのは、$Fil(n)$ の作り方である。以下のようにする。

$$\chi_0(n)=\begin{cases}0 & (n\equiv 0,2 \pmod 4)\\ 1 & (\text{それ以外のとき})\end{cases}$$

$$\chi(n)=\begin{cases}0 & (n\equiv 0,2 \pmod 4)\\ 1 & (n\equiv 1 \pmod 4)\\ -1 & (n\equiv 3 \pmod 4)\end{cases}\quad \text{とする。}$$

- $Fil(n) = \dfrac{1}{2}\{\chi_0(n) + \chi(n)\}$ とおくと、

$$Fil(n) = \begin{cases} 1 & (n \equiv 1 \pmod 4) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

$$\begin{aligned} S &= \sum_{p:\text{素数}} \sum_{r=1}^{\infty} Fil(p^r) \frac{1}{rp^{rs}} = \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \frac{1}{2}\{\chi_0(p^r) + \chi(p^r)\} \frac{1}{rp^{rs}} \\ &= \frac{1}{2} \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \chi_0(p^r) \frac{1}{rp^{rs}} + \frac{1}{2} \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \chi(p^r) \frac{1}{rp^{rs}} = \frac{1}{2}C + \frac{1}{2}D \end{aligned}$$

$$\begin{aligned} C &= \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \chi_0(p^r) \frac{1}{rp^{rs}} = \sum_{\substack{p:\text{素数} \\ p \neq 2}} \sum_{r=1}^{\infty} \frac{1}{rp^{rs}} \\ &= \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \frac{1}{rp^{rs}} - \sum_{r=1}^{\infty} \frac{1}{r \cdot 2^{rs}} = \log \zeta(s) - \log(1 - 2^{-s})^{-1} \end{aligned}$$

従って、$s \to 1 + 0$ のとき $C \to +\infty$

$$\begin{aligned} D &= \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \chi(p^r) \frac{1}{rp^{rs}} = \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \frac{1}{r} \left(\frac{\chi(p)}{p^s} \right)^r = \sum_{p:\text{素数}} \log \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \\ &= \log \prod_{p:\text{素数}} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} = \log \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \end{aligned}$$

- $Fil(n) = \dfrac{1}{2}\{\chi_0(n) - \chi(n)\}$ とおくと、

$$Fil(n) = \begin{cases} 1 & (n \equiv 3 \pmod 4) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

あとは、上と同様。//

注意　6 で割って余り 1 や 5 の素数が無限個あることも、上記と同様の方法で示すことができる。

4.2　5 で割った余りのとき

では、5 で割った余りの時の場合分けで素数を考える。これまでに比べて少し複雑になる。

定理４．２　5で割って余りが1の素数は無限個ある。

証明）$S=\sum_{\substack{p:\text{素数}\\ p^r\equiv 1 \pmod 5}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}$　とおく。

(I) $S=\sum_{\substack{p:\text{素数}\\ p\equiv 1 \pmod 5}}\frac{1}{p^s}+\sum_{\substack{p:\text{素数}\\ p^r\equiv 1 \pmod 5}}\sum_{r=2}^{\infty}\frac{1}{rp^{rs}}$

であり、第2の和は有限である。（前と同様)

(II) 「$n\equiv \pmod 5$ のときだけ生き残る関数 $Fil(n)$」 をうまく作ればよい。
天下り的ではあるが、次の「指標」を用いる。

$$\chi_0(n)=\begin{cases}0 & (n\equiv 0 \pmod 5)\\ 1 & (\text{それ以外のとき})\end{cases}$$

$$\chi(n)=\begin{cases}0 & (n\equiv 0 \pmod 5)\\ 1 & (n\equiv 1 \pmod 5)\\ i & (n\equiv 2 \pmod 5)\\ -i & (n\equiv 3 \pmod 5)\\ -1 & (n\equiv 4 \pmod 5)\end{cases}$$

とする。
注意：　mod 5 で 2 は原始根である。
（2 のべきで mod 5 のすべての元を表すことができる）

2の指数	0	1	2	3	4
mod 5	1	2	$2^2\equiv 4$	$2^3\equiv 3$	$2^4\equiv 1$
指標の値	1	i	$i^2=-1$	$i^3=-i$	$i^4=1$

このとき、 $\chi(ab)=\chi(a)\chi(b)$ が成り立つ。
さらに、 $Fil(n)=\frac{1}{4}\{\chi_0(n)+\chi(n)+\chi^2(n)+\chi^3(n)\}$ とおくと

- $Fil(0)=0$
- $Fil(1)=\frac{1}{4}(1+1+1+1)=1$
- $Fil(2)=\frac{1}{4}(1+i-i-1)=0$
- $Fil(3)=\frac{1}{4}(1-i-1+i)=0$
- $Fil(4)=\frac{1}{4}(1-1+1-1)=0$

従って、

$$Fil(n)=\begin{cases}1 & (n\equiv 1 \pmod 5)\\ 0 & (\text{それ以外のとき})\end{cases}$$

$$S=\sum_{p:素数}\sum_{r=1}^{\infty}Fil(p^r)\frac{1}{rp^{rs}}=\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{4}\left\{\chi_0(p^r)+\chi(p^r)+\chi^2(p^r)+\chi^3(p^r)\right\}\frac{1}{rp^{rs}}$$
$$=\frac{1}{4}\left\{\sum_{p:素数}\sum_{r=1}^{\infty}\chi_0(p^r)\frac{1}{rp^{rs}}+\sum_{p:素数}\sum_{r=1}^{\infty}\chi(p^r)\frac{1}{rp^{rs}}+\sum_{p:素数}\sum_{r=1}^{\infty}\chi^2(p^r)\frac{1}{rp^{rs}}+\sum_{p:素数}\sum_{r=1}^{\infty}\chi^3(p^r)\frac{1}{rp^{rs}}\right\}$$
$$=\frac{1}{4}(C+D+E+F)$$

$s\to 1+0$ について考える。

- $C=\sum_{p:素数}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}-\sum_{r=1}^{\infty}\frac{1}{r\cdot 5^{rs}}=\log\sum_{r=1}^{\infty}\frac{1}{n}-\log(1-5^{-1})=+\infty$
- $D=\log\sum_{r=1}^{\infty}\frac{\chi(n)}{n}$ であり、
  $$\sum_{r=1}^{\infty}\frac{\chi(n)}{n}=\sum_{k=0}^{\infty}\frac{1}{5k+1}+\sum_{k=0}^{\infty}\frac{i}{5k+2}+\sum_{k=0}^{\infty}\frac{-i}{5k+3}+\sum_{k=0}^{\infty}\frac{-1}{5k+4}$$
  $$=\sum_{k=0}^{\infty}\left(\frac{1}{5k+1}-\frac{1}{5k+4}\right)+i\sum_{k=0}^{\infty}\left(\frac{1}{5k+2}-\frac{1}{5k+3}\right)$$
  $$=3\sum_{k=0}^{\infty}\frac{1}{(5k+1)(5k+4)}+i\sum_{k=0}^{\infty}\frac{1}{(5k+2)(5k+3)}$$
  2 つの無限和は $\zeta(2)=\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$ と比較して収束することが示せる。よって、B は有限値となる。
- E,F も D と同様に有限値であることがわかる。

以上により、　$C\to;\infty$ が支配的となり、$S\to+\infty$ となる。

(I)、(II) により、$\sum_{\substack{p:素数\\ p\equiv 1\pmod 5}}\frac{1}{p}=+\infty$　が成り立ち、「5 で割って余りが 1 の素数は無限個ある」ことが証明された。

5 で割って余り 2 の素数については、$Fil(n)=\frac{1}{4}\{\chi_0(n)-i\chi(n)-\chi^2(n)+i\chi^3(n)\}$ とおくとよい。（どうしてそう置くのかということについては、後に説明することとする。）

- $Fil(0)=0$
- $Fil(1)=\frac{1}{4}(1-i-1+i)=0$
- $Fil(2)=\frac{1}{4}(1+1+1+1)=1$
- $Fil(3)=\frac{1}{4}(1-1+1-1)=0$

- $Fil(4) = \dfrac{1}{4}(1 + i - 1 - i) = 0$

従って、

$$Fil(n) = \begin{cases} 1 & (n \equiv 2 \pmod 5) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

5 で割って余り 3 の素数については、 $Fil(n) = \dfrac{1}{4}\{\chi_0(n) + i\chi(n) - \chi^2(n) - i\chi^3(n)\}$

5 で割って余り 4 の素数については、 $Fil(n) = \dfrac{1}{4}\{\chi_0(n) - \chi(n) + \chi^2(n) - \chi^3(n)\}$

を用いればよい。

5 関数 $Fil(n)$ について

5.1 $(\mathbb{Z}/5\mathbb{Z})^\times$ の場合

この場合、2 が生成元で $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3$ と位数 4 の巡回群になっている。それに合わせて、1 の 4 乗根として i を取り、$\chi(2) = i$ とおいて、後は $\chi(2^k) = \{\chi(2)\}^k = i^k \quad (k = 0, 1, 2, 3)$ とすればよいのである。

$1 + r + r^2 + \cdots r^{n-1} = \begin{cases} \dfrac{1 - r^n}{1 - r} & (r \neq 1) \\ n & (r = 1) \end{cases}$ であるから、

$$\chi_0(n) + \chi(n) + \chi^2(n) + \chi^3(n) = \begin{cases} 0 & (n \equiv 0, 2, 3, 4 \pmod 5) \\ 0 & (n \equiv 1 \pmod 5) \end{cases}$$

では、「5 で割って余り 2 の素数」の場合はどうするのか？

無限和を考えるときに、 $p^r \equiv 2 \pmod 5$ に関する和としていた。ところで、 $3 \cdot 2 \equiv 1 \pmod 5$ であるから、余り 2 のものに 3 をかけてやると余り 1 のものに結び付けることができる。すなわち、 $l = 3 \cdot p^r$ として、$\chi(l)$ を考えればよい。

このとき、 $\chi(l) = \chi(3 \cdot p^r) = \chi(3)\chi(p^r) = -i \cdot \chi(p^r)$

従って、 $Fil(n) = \dfrac{1}{4}\{\chi_0(n) - i\chi(n) - \chi^2(n) + i\chi^3(n)\}$ とおけば、「5 で割って余り 2 の時だけ生き残る関数」とできるのである。

余り 3 のときは、$2 \cdot 3 \equiv 1$ より、$l = 2 \cdot p^r, \quad \chi(l) = \chi(2 \cdot p^r)\chi(2)\chi(p^r) = i\chi(p^r)$

余り 4 のときは、$4 \cdot 4 \equiv 1$ より、$l = 4 \cdot p^r, \quad \chi(l) = \chi(4 \cdot p^r)\chi(4)\chi(p^r) = -\chi(p^r)$

を踏まえて $Fil(n)$ を作ればよい。

5.2 $(\mathbb{Z}/10\mathbb{Z})^\times$ の場合

10 以下で 10 と互いに素な自然数は、1,3,7,9 であるから $(\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$

このとき、$3^2 \equiv 9, 3^3 \equiv 7, 3^4 \equiv 1$ であるから、3 を生成元とする位数 4 の巡回群となる。

よって、$\chi(3) = i$ とおいて、あとは $(\mathbb{Z}/5\mathbb{Z})^\times$ の場合 と同様になる。

5.3 $(\mathbb{Z}/8\mathbb{Z})^\times$ の場合

$(\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\}$
このとき、$3^2 \equiv 1, 5^2 \equiv 1, 7^2 \equiv 1$ であるから、巡回群とならない。
（元の個数は 4 で $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$ と同じであるが。）
ことなる 2 つの数を掛けてみると $3 \cdot 5 \equiv 7$ であるから、
$1 \equiv 3^0 \cdot 5^0, \quad 3 \equiv 3^1 \cdot 5^0, \quad 5 \equiv 3^0 \cdot 5^1, \quad 7 \equiv 3^1 \cdot 5^1$　すなわち、$\{3^a \cdot 5^b \,|\, a = 0,1 \quad b = 0,1\}$ で表される。
従って、 $(\mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$A(3) = -1$, $B(5) = -1$ とおいて、$n = 1,3,5,7$ に対して以下の様に定める。

- $\chi_(n) = 1$ for $n = 1,3,5,7$
- $\chi_1(3^a \cdot 5^b) = A(3)^a$
- $\chi_2(3^a \cdot 5^b) = B(5)^b$
- $\chi_3(3^a \cdot 5^b) = A(3)^a \cdot B(5)^b$

関数の値を以下に表で整理する。

n	1	3	5	7
$\chi_0(n)$	1	1	1	1
$\chi_1(n)$	1	−1	1	−1
$\chi_2(n)$	1	1	−1	−1
$\chi_3(n)$	1	−1	−1	1

もちろん、8 と互いに素でない数（すなわち偶数）に対しては、値を 0 とする。

- 余り 1 のフィルタ関数は
  $Fil(n) = \frac{1}{4}\{\chi_0(n) + \chi_1(n) + \chi_2(n) + \chi_3(n)\}$
- 余り 3 のフィルタ関数は、 $3 \cdot 3 \equiv 1$ を踏まえて 3^1 のところに -1 を掛けて
  $Fil(n) = \frac{1}{4}\{\chi_0(n) - \chi_1(n) + \chi_2(n) - \chi_3(n)\}$
- 余り 5 のフィルタ関数は、 $5 \cdot 5 \equiv 1$ を踏まえて 5^1 のところに -1 を掛けて
  $Fil(n) = \frac{1}{4}\{\chi_0(n) + \chi_1(n) - \chi_2(n) - \chi_3(n)\}$
- 余り 7 のフィルタ関数は、 $3^1, 5^1$ のところに -1 を掛けて
  $Fil(n) = \frac{1}{4}\{\chi_0(n) - \chi_1(n) - \chi_2(n) + \chi_3(n)\}$

これらを用いて、前と同様な考察をすれば、8 で割った余りが 1,3,5,7 の素数がそれぞれ無限個あることがわかる。

具体的な数についての考察はこのあたりにして、一般論について述べることにする。

6　指標

G : 有限アーベル群、　$\mathbb{C}^\times = \{z \in \mathbb{C} \,|\, |z| = 1\}$ とするとき、
$\chi : G \to \mathbb{C}^\times$: 準同型　を「有限群 G 上の指標（character）」と呼ぶ。
ただし、準同型というのは、 $\forall a, b \in G$ について、 $\chi(ab) = \chi(a)\chi(b)$ が成り立つことである。
前節で扱った指標 χ は、 $G = (\mathbb{Z}/4\mathbb{Z})^\times, (\mathbb{Z}/5\mathbb{Z})^\times, (\mathbb{Z}/10\mathbb{Z})^\times, (\mathbb{Z}/8\mathbb{Z})^\times$ としたものである。

補題６．１　$\chi(1) = 1$ を満たす。

証明）$\chi(1^2) = \chi(1)\chi(1)$ であるから、 $\chi(1) = \chi(1)^2$　ゆえに $\chi(1) = 0, 1$
$|\chi(1)| = 1$ より $\chi(1) = 1$ //

定義（双対群）　有限群 G 上の指標全体の集合を $\hat{G} = \{\chi \,|\, \chi$は G 上の指標 $\}$ とする。
このとき、任意の $\chi_1, \chi_2 \in \hat{G}$ について、 $\chi_3(g) := \chi_1(g)\chi_2(g)$ for $\forall g \in G$ で定めると、
χ_3 は G 上の指標となる。これを「 χ_1 と χ_2 の積」と言い、 $\chi_1\chi_2$ で表す。
また、 $\chi \in \hat{G}$ について、 χ^{-1} を $\chi^{-1}(g) = \{\chi(g)\}^{-1}$ for $\forall g \in G$ で定めると、 χ^{-1} は G 上の指標となる。これを「 χ の逆元」と言う。それは $\chi\chi^{-1} = \chi_0$ を満たすからである。
これらにより、 $\hat{G}$ は群をなす。これを G **の双対群** と言う。

具体例で少し考えてみる。

- $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\} = \{2^0, 2^1, 2^2, 2^3\}$ の場合
  $\chi \in \hat{G}$ について、 $\chi(2) = \zeta$ とおくと、
  $\chi(1) = 1, \quad \chi(3) = \chi(2^3) = \chi(2)^3 = \zeta^3, \quad \chi(4) = \chi(2^2) = \chi(2)^2 = \zeta^2$
  さらに、 $\chi(1) = \chi(2^4) = \chi(2)^4$ より $1 = \zeta^4$。 したがって、 $\zeta = \pm 1, \pm i$
  逆に、この 4 つの値を $\chi(2)$ の値 ζ に設定すると、 $\chi(3) = \zeta^3, \chi(4) = \zeta^2$ とすることにより指標を作ることができる。

$\chi_0(2)=1,\quad \chi_1(2)=-1,\quad \chi_2(2)=i,\quad \chi_3(2)=-i$ として以下の表のとおりとなる。

g	1	2	3	4
$\chi_0(g)$	1	1	1	1
$\chi_1(g)$	1	-1	-1	1
$\chi_2(g)$	1	i	$-i$	-1
$\chi_3(n)$	1	$-i$	i	-1

ここで、$\chi_1=\chi_2^2,\quad \chi_3=\chi_2^3$ より、 $\hat{G}$ は位数 4 の巡回群で G と同型。

- $G=(\mathbb{Z}/10\mathbb{Z})^\times$ のときも同様に $G\simeq\hat{G}$。
- $G=(\mathbb{Z}/8\mathbb{Z})\simeq(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ のとき
  $\chi(g)=\chi(3^a\cdot5^b)=\chi(3)^a\cdot\chi(5)^b=\zeta_1^a\cdot\zeta_2^b$ （ただし、 $\zeta_1=\chi(3),\zeta_2=\chi(5)$）
  $\chi_1^2=\chi_2^2=1$ を満たすから、$\zeta_1=\pm1,\quad \zeta_2=\pm1$
  逆に、 ζ_1,ζ_2 の組み合わせを 4 通り考え、 $\chi(3^a\cdot5^b)=\zeta_1^a\zeta_2^b$ で定めると、これは G 上の指標を与える。
  従って、 $\hat{G}\simeq\{(\zeta_1,\zeta_2)\,|\,\zeta_1=\pm1,\zeta2=\pm1\}\simeq(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})\simeq G$

補題６．２ $G\simeq\hat{G}$ が成り立つ。

証明）一般に有限アーベル群は
$G=\{g_1^{e_1}\cdot g_2^{e_2}\cdot\cdots\cdot g_k^{e_k}\,|\,g_i^{N_i}=1\quad$ かつ $\quad 1\leqq i<N_i\quad$ について $g_i^n\neq1\}$
$\simeq(\mathbb{Z}/N_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/N_k\mathbb{Z})$
となることが知られている。（ここでは証明を省略する。）
$\chi\in\hat{G}$ について、 $\chi(g_i)=\zeta_i$ とおくと、$\chi(g_i^{N_i})=\{\chi(g_i)\}^{N_i},\quad \chi(1)=\zeta_i^{N_i}$
従って、 $\zeta_i^{N_i}=1\quad(i=1,2,\cdots,k)$ となる。すなわち、ζ_i は 1 の N_i 乗根である。
逆に、$\zeta_i^{N_i}=1\quad(i=1,2,\cdots,k)$ を満たす数の組を任意にとり、$g\in G$ が $g=g_1^{e_1}g_2^{e_2}\cdots g_k^{e_k}$ であるときに、 $\chi(g)=\zeta_1^{e_1}\zeta_2^{e_2}\cdots\zeta_k^{e_k}$ と定めると、 χ は G 上の指標となる。
$\therefore\hat{G}\simeq\left\{(\zeta_1,\cdots,\zeta_k)\,|\,\zeta_i^{N_i}=1\quad(1\leqq i\leqq k)\right\}\simeq(\mathbb{Z}/N_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/N_k\mathbb{Z})\simeq G$ //

系 元の個数を考えて、特に $|G|=|\hat{G}|$

補題６．３ $\chi:G\to\mathbb{C}^\times$ を指標とするとき、

(1) $\chi=\chi_0$ ならば $\displaystyle\sum_{g\in G}\chi(g)=|G|$

(2) $\chi\neq\chi_0$ ならば $\displaystyle\sum_{g\in G}\chi(g)=0$

証明）(1) は自明
(2) について、$\chi\neq\chi_0$ より、$^\exists g_1\in G$ s.t. $\chi(g_1)\neq1$

- このとき、$\sum_{g\in G}\chi(g_1g)=\sum_{g\in G}\chi(g)$
  $\because) g,g'\in G\quad g_1g=g_1g'$ とすると、両辺に g_1^{-1} を掛けて $g=g'$ となる。
  従って、$^{\#}\{g_1g\,|\,g\in G\}=^{\#}\{g\in G\}$ 。　$\therefore \{g_1g\,|\,g\in G\}=G$ //

- 従って、$\chi(g_1)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(g),\quad \{\chi(g_1)-1\}\sum_{g\in G}\chi(g)=0$
  $\chi(g_1)-1\neq 0$ より、$\sum_{g\in G}\chi(g)=0$　(証明終)

補題６．４ G を有限群、$\hat{G}$ を G の指標群とするとき、

(1) $\sum_{\chi\in\hat{G}}\chi(1)=|G|$

(2) $g_1\in G,\ g_1\neq 1$ ならば $\sum_{\chi\in\hat{G}}\chi(g_1)=0$

証明）(1) は自明
(2) について

- $g_1\neq 1$ のとき、$^{\exists}\chi_1\in\hat{G}$ s.t. $\chi_1(g_1)\neq 1$
  $\because)^{\forall}\chi\in\hat{G}$ について、$\chi(g_1)=1$ であると仮定して矛盾を導く。
  $h,k\in G$ が $<g_1>=\{1,g_1,g_1^2,\cdots\}$ で同値 $h\sim k$ とは、$^{\exists}l\in\mathbb{Z}$ s.t. $h=g_1^lk$ となることとする。そして、G をこの同値で類別したものを $G_1=G/<g_1>$ とする。
  (例. $G=(\mathbb{Z}/5\mathbb{Z})^{\times}$で、$g_1=4$ のとき、$<g_1>=\{1,4\}$,　$2\cdot 4\equiv 3$ より、$G_1=G/<g_1>=\{1,2$
  $\forall\chi\in\hat{G}$ について、$h\sim k$ ならば、$\chi(h)=\chi(g_1^lk)=\chi(g_1)^l\cdot\chi(k)=\chi(k)$
  ということは、χ は G_1 上の指標であると言ってよい。その個数は全部で $|G_1|$ である。しかるに、G 上の指標は $|G|$ 個なければならず、$|G_1|<|G|$ であることから足りないことになる。矛盾。//

- 上の χ_1 について、$\{\chi_1\chi\,|\,\chi\in\hat{G}\}=\hat{G}$ であることが示せるので、
  $\sum_{\chi\in\hat{G}}\chi_1\chi(g_1)=\sum_{\chi\in\hat{G}}\chi(g_1),\quad \chi_1(g_1)\sum_{\chi\in\hat{G}}\chi(g_1)=\sum_{\chi\in\hat{G}}\chi(g_1),\quad \{\chi_1(g_1)-1\}\sum_{\chi\in\hat{G}}\chi(g_1)=0$
  $\chi_1(g_1)-1\neq 0$ より、$\sum_{\chi\in\hat{G}}\chi(g_1)=0$　（証明終）

命題６．１　N : 自然数、$G=(\mathbb{Z}/N\mathbb{Z})^{\times}$ 、
$\varphi(N)=^{\#}\{1\leqq x\leqq N-1\,|\,N$ と x は互いに素 $\}$ のとき、
$Fil(g):=\dfrac{1}{\varphi(N)}\sum_{\chi\in\hat{G}}\chi(g)$ とおくと、

$$Fil(g)=\begin{cases}1 & (g\equiv 1\ (\mathrm{mod}\ N))\\ 0 & (\text{それ以外のとき})\end{cases}$$

証明）　補題から容易に導かれる。

補題６．５　N : 自然数、$1 \leqq r \leqq N-1$、$(N,r)=1$ のとき、$^{\exists}r'$　s.t. $rr' \equiv 1 \pmod N$
証明）$(N,r)=1$ より、$^{\exists}a, b \in \mathbb{Z}$　s.t. $aN+br=1$ 。このとき、$br \equiv 1 \pmod N$
この b について、$^{\exists}r'$,　$1 \leqq r' \leqq N-1$,　$b \equiv r' \pmod N$,　$r'r \equiv 1 \pmod N$ //

この r' を r^{-1} と記す。

さて、$G=(\mathbb{Z}/N\mathbb{Z})^{\times}$,　$k \in G$ のとき、$Fil(n) := \dfrac{1}{\varphi(N)} \displaystyle\sum_{\chi \in \hat{G}} \chi(k^{-1}n)$ とおくと、

$$Fil(n) = \begin{cases} 1 & (n \equiv k \pmod N) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

7　算術級数定理の証明

$s>1$ に対して、

$\Phi(s) = \displaystyle\sum_{\substack{p:\text{素数} \\ p^r \equiv k \pmod N}} \sum_{r=1}^{\infty} \frac{1}{rp^{rs}}$　とおく。そして、$s \to 1+0$ の時の極限について、和を 2 通りに変形して考えてみるのである。

(I) $\Phi(s) = \displaystyle\sum_{\substack{p:\text{素数} \\ p \equiv k \pmod N}} \frac{1}{p^s} + \sum_{\substack{p:\text{素数} \\ p^r \equiv k \pmod N}} \sum_{r=2}^{\infty} \frac{1}{rp^{rs}}$

上の第 2 の和で $s=1$ を代入したものを A とおくと、

$$0 < A < \sum_{p:\text{素数}} \sum_{r=2}^{\infty} \frac{1}{rp^r} < \sum_{p:\text{素数}} \sum_{r=2}^{\infty} \frac{1}{2p^r} = \sum_{p:\text{素数}} \frac{1}{2} \frac{\frac{1}{p^2}}{1-\frac{1}{p}} = \sum_{p:\text{素数}} \frac{1}{2} \frac{1}{p(p-1)}$$
$$< \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2} \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = \frac{1}{2}$$

よって、$s \to 1+0$ のとき、第 2 の和は有限な値に収束する。

(II) $\Phi(s) = \displaystyle\sum_{p:\text{素数}} \sum_{r=1}^{\infty} Fil(k^{-1}p^r) \frac{1}{rp^{rs}} = \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \left\{ \frac{1}{\varphi(N)} \sum_{\chi \in \hat{G}} \chi(k^{-1}p^r) \right\} \frac{1}{rp^{rs}}$

$$= \frac{1}{\varphi(N)} \sum_{\chi \in \hat{G}} \chi(k^{-1}) \sum_{p:\text{素数}} \sum_{r=1}^{\infty} \frac{\chi(p^r)}{rp^{rs}} = \frac{1}{\varphi(N)} \sum_{\chi \in \hat{G}} \left\{ \chi(k^{-1}) \sum_{p:\text{素数}} \log \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \right\}$$

$$= = \frac{1}{\varphi(N)} \sum_{\chi \in \hat{G}} \left\{ \chi(k^{-1}) \log \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \right\}$$

$$= \frac{1}{\varphi(N)} \log \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} + \frac{1}{\varphi(N)} \sum_{\chi \neq \chi_0} \left\{ \chi(k^{-1}) \log \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \right\}$$

ここで、

- 第1の和が、 $s \to 1+0$ のとき $+\infty$ に発散する。
- $\chi \neq \chi_0$ のとき、 $\lim_{s\to 1+0} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ が0以外の有限な値に収束する。

ことを示す。

定理７．１ $L(s,\chi_0) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s}$ は $Re(s) > 1$ で一様絶対収束し、s の正則関数を定義する。そして、$s=1$ において1位の極を持つ。

証明） $L(s,\chi_0) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = \prod_{p:\text{素数}} \frac{1}{1-\frac{\chi_0(p)}{p^s}} = \prod_{\substack{p:\text{素数} \\ p\not| N}} \frac{1}{1-\frac{\chi(p)}{p^s}}$

$$= \prod_{p|N} \left(1-\frac{1}{p^s}\right) \prod_{p:\text{素数}} \frac{1}{1-\frac{1}{p^s}} = \prod_{p|N} \left(1-\frac{1}{p^s}\right) \zeta(s)$$

あとは、$\zeta(s)$ の性質から従う。//

これにより、先の第1の和について、「 $s \to 1+0$ のとき $+\infty$ に発散する。」が示された。

補題７．１ $A(M) := \sum_{n=1}^{M} a_n$ とし、 $\limsup_{M\to\infty} \frac{|A(M)|}{M^\sigma} < +\infty$ ならば、$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ は、$s > \sigma$ において一様収束する。

（証明は後回しにする。）

補題７．２ $\chi \neq \chi_0$ のとき、 $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ は $s > 0$ で一様収束する。

証明）$A(M) = \sum_{n=1}^{M} \chi(n)$ とおくと、 $A(N) = \sum_{n=1}^{N} \chi(n) = 0$ $(\chi \neq \chi_0)$ であるから、
$A(2N) = A(3N) = \cdots = 0$
$M = kN + r$ $(0 \leqq r < N)$ とすると、

- $r = 0$ のとき、 $A(M) = A(kN) = 0$
- $1 \leqq < N$ のとき、$A(M) = A(kN+r) = A(kN) + \sum_{n=kN+1}^{kN+r} \chi(n) = 0 + \sum_{n=1}^{r} \chi(n)$

  $\therefore |A(M)| \leqq \sum_{n=1}^{r} |\chi(n)| \leqq \sum_{n=1}^{r} 1 = r < N$

  $\therefore \limsup_{M\to+\infty} \frac{|A(M)|}{M^0} < N$ 。補題6より補題7の主張は正しい。//

これにより、「第２の和で $\chi \neq \chi_0$ のとき、$\lim_{s\to 1+0}\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ が有限な値に収束する。」ことは示された。あと、それが 0 ではないことを示すと、 log をとっても有限な値になることがわかる。それがなかなか大変なのである。

補題７から次が言える。

定理７．２ $\chi \neq \chi_0$ のとき、$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ は $Re(s)>0$ において一様絶対収束し、 s の正則関数を定義する。

これを $L(s,\chi)$ と記して、Dirichlet の L-函数と呼ぶ。

Euler 積では、$L(s,\chi)=\prod_{p:素数}\left(1+\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{p^{2s}}+\cdots\right)=\prod_{p:素数}\frac{1}{1-\frac{\chi(p)}{p^s}}$

定理７．３ $\chi \neq \chi_0$ のとき、$L(1,\chi)\neq 0$

証明）$L(1,\chi_1)=0$ を満たす指標 χ_1 があったと仮定して矛盾を導く。

$F(s):=\prod_{\chi\in\hat{G}}L(s,\chi)$ とおく。

上の積の中には $L(s,\chi_0)$ が含まれており、それは $s=1$ において 1 位のを持つが、その他は $s=1$ で正則であり、かつ $L(1,\chi_1)=0$ であるから、極は打ち消される。そのため、 $F(s)$ は $s=1$ において正則になる。

$s>1$ のとき、

$$\log F(s)=\sum_{\chi\in\hat{G}}\log L(s,\chi)=\sum_{\chi\in\hat{G}}\log\prod_{p:素数}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}=\sum_{\chi\in\hat{G}}\sum_{p:素数}\sum_{r=1}^{\infty}\frac{\chi(p^r)}{rp^{rs}}$$

$$=\sum_{p:素数}\sum_{r=1}^{\infty}\left\{\sum_{\chi\in\hat{G}}\chi(p^r)\right\}\frac{1}{rp^{rs}}=\varphi(N)\sum_{p:素数}\sum_{\substack{r=1\\ p^r\equiv 1 \pmod N}}^{\infty}\frac{1}{rp^{rs}}>0\quad \text{for } r>1$$

$\therefore s>1$ のとき $F(s)>1$

このため、もし、 χ_1 以外にも $L(s,\chi)=0$ を満たす指標があると $\lim_{s\to 1+0}F(s)=0$ となり、上の結果に矛盾する。従って、 $L(s,\chi)=0$ を満たす指標は χ_1 以外にありえない。

Claim　χ_1 は実指標である。

$\because$ ）$L(1,\overline{\chi_1})=\sum_{n=1}^{\infty}\frac{\overline{\chi(n)}}{n}=\overline{\left\{\sum_{n=1}^{\infty}\frac{\chi_1(n)}{n}\right\}}=\overline{L(1,\chi_1)}=0$

よって、 $\overline{\chi_1}$ も $L(1,\chi)=0$ を満たす指標である。そのような指標は、 χ_1 のみであるから、 $\overline{\chi_1}=\chi_1$ //

$Re(s)>1$ に対して、 $\Phi(s):=\frac{L(s,\chi_0)L(s,\chi_1)}{L(2s,\chi_0)}$ とおく。

$s=1$ のところを考える。分母は、$L(2,\chi_0)\neq 0$

分子では、 $L(s,\chi_0)$ の極と $L(s,\chi_1)$ の零が打ち消しあって正則である。
よって、 $s=1$ において $\Phi(s)$ は正則である。そのため、 $Re(s)>\dfrac{1}{2}$ で正則である。

Euler 積により

$$\Phi(s)=\prod_{p:\text{素数}}\frac{1-\dfrac{\chi_0(p)}{p^{2s}}}{\left\{1-\dfrac{\chi_0(p)}{p^s}\right\}\left\{1-\dfrac{\chi_1(p)}{p^s}\right\}}$$

$$=\prod_{\substack{p|N\\ \text{素数}}}\frac{1-0}{(1-0)(1-0)}\times\prod_{\substack{p\not|N\\ \text{素数}}}\frac{1-\dfrac{1}{p^{2s}}}{\left(1-\dfrac{1}{p^s}\right)\left\{1-\dfrac{\chi_1(p)}{p^s}\right\}}$$

$$=\prod_{\substack{p\not|N\\ \text{素数}}}\frac{1+\dfrac{1}{p^s}}{1-\dfrac{\chi_1(p)}{p^s}}=\prod_{\chi_1(p)=1}\frac{1}{1-\dfrac{1}{p^s}}=\prod_{\chi_1(p)=1}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right)$$

$\therefore\quad \Phi(s)=\displaystyle\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ と Dirichlet 級数で表した時に、すべての $a_n\geqq 0$

$\Phi(s)$ の $s=2$ におけるテーラー展開を考えると、 $s>\dfrac{1}{2}$ で収束するはずなので、
$|s-2|<\dfrac{3}{2}$ において、

$$\Phi(s)=\sum_{k=0}^{\infty}\frac{\Phi^{(k)}(2)}{k!}(s-2)^k$$

ここで、 $\dfrac{d}{ds}\dfrac{1}{n^s}=n^{-s}\cdot\log n\cdot(-s)'=-\dfrac{\log n}{n^s}$ より、 $\dfrac{d^k}{ds^k}\dfrac{1}{n^s}=\dfrac{(-\log n)^k}{n^s}$

$$\Phi(s)=\sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{n=1}^{\infty}\frac{(-\log n)^k a_n}{n^2}\right)(s-2)^k=\sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{n=1}^{\infty}\frac{(\log n)^k a_n}{n^2}\right)(2-s)^k$$

$a_n\geqq 0\quad$ for $\hat{}\,\forall n$ より、 $\Phi(s)$ は、 $\dfrac{1}{2}<s<2$ において単調減少。
よって、 $\Phi(2)<\Phi(s)\quad$ for $\quad\dfrac{1}{2}<s<2$

$$\Phi(s)=\prod_{\chi_1(p)=1}\frac{1}{1-\dfrac{1}{p^2}}>1\qquad\therefore\quad\Phi(s)>1\quad\text{for}\quad\frac{1}{2}<s<2$$

しかるに、 $s\to\dfrac{1}{2}$ のとき、

- $\Phi(s)$ の分子 $L\left(\dfrac{1}{2},\chi_0\right)L\left(\dfrac{1}{2},\chi_1\right)$ は有限値である。
- $\Phi(s)$ の分母で $\displaystyle\lim_{s\to\frac{1}{2}+0}L(2s,\chi_0)=\lim_{t\to 1+0}\prod_{p|N}\left(1-\frac{1}{p^t}\right)\times\zeta(t)=+\infty$

従って、 $\displaystyle\lim_{s\to\frac{1}{2}+0}\Phi(s)=0$

これは、先に示した $\Phi(s)>1\quad$ for $\quad\dfrac{1}{2}<s<2$ に反する。よって、 $L(1,\chi_1)=0$

を満たす指標 χ_1 は存在しない。　　（定理３の証明終わり）

これにより、「第２の和で $\chi \neq \chi_0$ のとき、$\lim_{s\to 1+0}\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ が０以外の有限な値に収束する。」ことは示された。

定理７．４　（算術級数定理）

$N, a \in \mathbb{N}$ で N と a が互いに素のとき、
算術級数（等差数列）$\{a+kN \,|\, k=0,1,2,\cdots\}$ の中に無限個の素数がある。

証明）先に考えた $\Phi(s)$ の２通りの和の変形を振り返る。

(I)　$\Phi(s) = \sum_{\substack{p:\text{素数}\\ p\equiv k \pmod N}} \frac{1}{p^s} + \sum_{\substack{p:\text{素数}\\ p^r\equiv k \pmod N}} \sum_{r=2}^{\infty}\frac{1}{rp^{rs}}$

$s \to 1+0$ のとき、第２の和は有限となるのであった。

(II)　$\Phi(s) = \frac{1}{\varphi(N)}\log\sum_{n=1}^{\infty}\frac{\chi_0(n)}{n^s} + \frac{1}{\varphi(N)}\sum_{\chi\neq\chi_0}\left\{\chi(k^{-1})\log\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\right\}$

$s \to 1+0$ のとき、第１の和 $\to +\infty$ 、第２の和は有限値であった。

これらのことから、(I) の第１の和で $s \to 1+0$ として、$\sum_{\substack{p:\text{素数}\\ p\equiv k \pmod N}} \frac{1}{p} = +\infty$

$p \equiv k \pmod N$ を満たす素数が有限個しかなかったら、その逆数の和は有限値となるから、上式は成り立たない。従って、そのような素数は無限個ある。（証明終わり）

以上、D.B.Zagier 「Zetafunktionen und quadratische Körper」 Springer-Verlag（日本語訳は岩波書店「数論入門」　片山孝次　訳）を学習した際のメモである。お盆前に、手書きの原稿はできたのであるが、TeX に打ち込むのに時間がかかった。