算術級数定理への入口

平成27年11月28日(土)「きときと数学研修会」話題提供
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

定理1 素数は無限個存在する.

$2+1=3$, $2\cdot3+1=7$, $2\cdot3\cdot5+1=31$, $2\cdot3\cdot5\cdot7+1=211$
$2\cdot3\cdot5\cdot7\cdot11+1=2311$ $2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031=59\times509$

証明) ユークリッドによる証明。背理法
素数が有限個しかなく, それらが $P_1=2, P_2=3, \cdots, P_k$ で全てであったとする。
このとき $N=P_1\cdot P_2\cdot\cdots\cdot P_k+1$ とおくと N は $P_1, \cdots, P_k$ のいずれでも割り切れない。
従って N の素因数は $P_1, P_2, \cdots, P_k$ と異なることになり, 仮定に反する。 //

定理2 4で割って3余る素数は無限個存在する.

$4\cdot3-1=11$ $4\cdot7-1=83$ $4\cdot7\cdot11-1=923=13\cdot71$
$4\cdot3\cdot7\cdot11\cdot19-1=17555=5\cdot3511$

証明) 背理法
4で割って3余る素数が有限個しかなく, それらが $P_1=3, P_2=7, \cdots, P_k$ で全てであったとする
このとき $N=4P_1\cdot P_2\cdot\cdots\cdot P_k-1$ とおくと N は4で割って3余る自然数で, 明らかに3より大きい。
また, $P_1, P_2, \cdots, P_k$ のいずれでも割り切れない. 仮定より, 4で割って3余る素数はそれ以外に
無いので N の素因数は全て4で割って1余るものばかりということになる. …Ⓐ
ところで $a=4l+1$, $b=4m+1$ とすると $ab=4(4lm+l+m)+1$ であることから
4で割って1余る数の積は4で割って1余ることになる。Ⓐより N は4で割って1余る.
上で N は4で割って3余るとなることに矛盾する。 //

定理3 4で割って1余る素数は無限個ある.

$4\cdot5^2+1=101$ $4\cdot5^2\cdot13^2+1=16901$
$4\cdot5^2\cdot13^2\cdot17^2+1=4884101$

証明) 背理法
4で割って1余る素数が有限個しかなく, それらが $P_1, P_2, \cdots, P_k$ で全てであったとする.
このとき $N=4P_1^2P_2^2\cdots\cdots P_k^2+1$ とおいて考える.

$4\cdot5^2\cdot13^2\cdot17^2\cdot29^2+1=4,107,528,101$ ← 素数かどうか?

(i) N は4で割って1余る。
(ii) N は $P_1, P_2, \cdots, P_k$ のいずれでも割り切れない。仮定より N の素因数は4で割って3余るものばかりである.
(iii) $N=(2P_1P_2\cdots P_k)^2+1$ $x=2P_1P_2\cdots\cdot P_k$ とおくと $N=x^2+1$.
ここで N の素因数の1つを p とすると $N\equiv0 \pmod p$ より $x^2+1\equiv0 \pmod p$
$\therefore x^2\equiv-1 \pmod p$ $\therefore x^4\equiv1 \pmod p$

ここで少し一般論になるが $(\mathbb{Z}/p\mathbb{Z})^\times=\{1,2,\cdots,p-1\}$ は積について位数 $p-1$ の有限群である.
そして $\forall x\in(\mathbb{Z}/p\mathbb{Z})^\times$, $x^{p-1}\equiv1 \pmod p$ である (フェルマーの小定理)
$p-1$ を4で割った商を q, 余りを r とすると $0\le r<4$, $p-1=4q+r$
$x^{p-1}=x^{4q+r}=(x^4)^q\times x^r\equiv1^q\cdot x^r$ $\therefore x^r\equiv1 \pmod p$
・$r=1$ とすると $x\equiv1$ より $x^2\equiv-1$ に反する. $r=2$ も $x^2\equiv-1$ に反する.

$r=3$ とすると $x^3=x^2\cdot x\equiv -1\cdot x\equiv 1$ $\therefore x\equiv -1$. これは $x^2\equiv -1$ に反する

以上より $r=0$ となる。 すると $p-1=4q$ $\underline{p=4q+1}$ … p が4で割って3余ることに矛盾//

紀元前3世紀ごろにユークリッドが「素数は無限個存在する」ことを証明した方法と類似の方法で4で割って余り1の素数，余り3の素数はともに無限個あることを示すことができた。
しかし，3で割って1余る素数が無限個あるかどうかは，このような方法で証明することはできそうにない。
別の方法で示されるのだが，それには解析関数を使っていくのが不思議な感じがする．

補題1 $\boxed{|x|<1 \text{ のとき } -\log(1-x)=\sum_{r=1}^{\infty}\frac{x^r}{r}}$

証明) 数Ⅲで $\frac{1}{1-x}=1+x+x^2+\cdots$ $(|x|<1)$ を示している．
これは絶対収束であり，両辺を積分するとき，右辺では項別積分してもよいことを大学で学ぶので

$$-\log(1-x)=x+\frac{1}{2}x^2+\frac{1}{3}x^3+\cdots$$ //

これを用いて 定理1の別証を与えるのだが 二重和の順序の入れ換えなどは，ここでは厳密なところにこだわらずに進めていくことにする（「絶対収束」により，大丈夫なのである）

定理1の別証) $S=\sum_{r=1}^{\infty}\sum_{p:\text{素数}}\frac{1}{rp^r}$ を考える．

（↑全ての素数について和を考えるという意味）

注意 厳密には $F(s)=\sum_{r=1}^{\infty}\sum_{p:\text{素数}}\frac{1}{rp^{rs}}$ を $s>1$ で考えて絶対収束としておき，$s\to 1+0$ を考えていくのであるが…

Sを以下で(Ⅰ)，(Ⅱ)の2通りの変形で計算を進め，結果を比較する

(Ⅰ) 和を $r=1$ のところと，$r\geq 2$ のところに分けて考える．（$r\geq 2$ のところは「おとなしい和」になる。）

$S=\sum_{p:\text{素数}}\frac{1}{rp^r}+\sum_{r=2}^{\infty}\sum_{p:\text{素数}}\frac{1}{rp^r}=A+B$ とする

$$0<B<\sum_{r=2}^{\infty}\sum_{p:\text{素数}}\frac{1}{2p^r}=\frac{1}{2}\sum_{p:\text{素数}}\sum_{r=2}^{\infty}\frac{1}{p^r}=\frac{1}{2}\sum_{p:\text{素数}}\frac{\frac{1}{p^2}}{1-\frac{1}{p}}=\frac{1}{2}\sum_{p:\text{素数}}\frac{1}{p(p-1)}$$

$$<\frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{n(n-1)}=\frac{1}{2}\times\lim_{N\to\infty}\sum_{n=2}^{N}\left(\frac{1}{n-1}-\frac{1}{n}\right)=\frac{1}{2}\times\lim_{N\to\infty}\left(1-\frac{1}{N}\right)=\frac{1}{2}$$

$\therefore$ Bは正の有限値である。 $\underline{S=A+(\text{正の有限値})}$

(Ⅱ) Sを $-\log(1-x)$ の形へ

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

ここで $\prod_{p:\text{素数}}\frac{1}{1-\frac{1}{p}}=\prod_{p:\text{素数}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=\sum_{n=1}^{\infty}\frac{1}{n}=+\infty$ $\therefore \underline{S=+\infty}$

（数Ⅲで証明できる）

(I), (II) より　$A+$ (正の有限値) $=+\infty$　　$\therefore A=+\infty$

$\therefore \underline{\sum_{p:素数} \frac{1}{p} = +\infty}$　　もし素数が有限個しかなかったら，左辺は有限individで有限値

$\therefore$ 素数は無限個ある. //

ポイントは $\sum_{p:素数} \frac{1}{p} = +\infty$ を示すために，ソレ方が $\sum_{r=1}^{\infty} \sum_{p:素数} \frac{1}{rp^r}$ を考えることである.

この方法で進めていく.

定理4　3で割って1余る素数は無限個ある.

証明)　$\sum_{\substack{p:素数で \\ 3で割って1余る}} \frac{1}{p} = +\infty$ を示すことができればよい　　$\frac{1}{7}+\frac{1}{13}+\frac{1}{19}+\frac{1}{31}+\cdots = +\infty$

⇓

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

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

$0 < B < \sum_{\substack{p:素数 \\ p^r \equiv 1 \pmod 3}} \sum_{r=2}^{\infty} \frac{1}{2p^r} = \frac{1}{2} \sum_{\substack{p:素数 \\ p^r \equiv 1 \pmod 3}} \frac{\frac{1}{p^2}}{1-\frac{1}{p}} = \frac{1}{2} \sum_{\substack{p:素数 \\ p^r \equiv 1 \pmod 3}} \frac{1}{p(p-1)}$

$< \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2}$　(前と同じ計算)　$\therefore \underline{S = A+ (正の有限値)}$

(II)　$-\log(1-x)$ の形にしたいが「$p^r \equiv 1 \pmod 3$」と条件付きの和になっているところがめんどうである。条件の無い「$\sum_{p:素数}$」という和にしたいので工夫する

そのためには「3で割って1余る数」だけを取り出す次の関数があるとよい.

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

すると

$$\sum_{\substack{p:素数 \\ p^r \equiv 1 \pmod 3}} \frac{1}{rp^r} = \sum_{p:素数} \frac{Fil(p^r)}{rp^r}$$ とできる.

この関数 $Fil(n)$ の作り方は以下のように $\chi_0(n)$, $\chi(n)$ という2つの関数を用いる.（「指標」と呼ばれる関数）

$\cdot \chi_0(n)=\begin{cases}0 & (n\equiv 0 \pmod 3)\\ 1 & (n\equiv 1,2 \pmod 3)\end{cases}$ $\cdot \chi(n)=\begin{cases}0 & (n\equiv 0 \pmod 3)\\ 1 & (n\equiv 1 \pmod 3)\\ -1 & (n\equiv 2 \pmod 3)\end{cases}$

補題2 $\chi_0(ab)=\chi_0(a)\chi_0(b)$, $\chi(ab)=\chi(a)\chi(b)$ が成り立つ

証明) 乗積表

b \ a	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

により 代入, 計算して示せる. //

補題3 $Fil(n)=\frac{1}{2}\{\chi_0(n)+\chi(n)\}$ とおくと $Fil(n)=\begin{cases}1 & (n\equiv 1 \pmod 3)\\ 0 & (n\equiv 0,2 \pmod 3)\end{cases}$

証明) $Fil(0)=\frac{1}{2}(0+0)=0$, $Fil(1)=\frac{1}{2}(1+1)=1$, $Fil(2)=\frac{1}{2}(1-1)=0$ //

これを用いて S を計算する

$$S=\sum_{r=1}^{\infty}\sum_{p:素数}\frac{Fil(p^r)}{rp^r}=\sum_{r=1}^{\infty}\sum_{p:素数}\frac{\frac{1}{2}\{\chi_0(p^r)+\chi(p^r)\}}{rp^r}$$

$$=\frac{1}{2}\sum_{p:素数}\left[\sum_{r=1}^{\infty}\frac{\{\chi_0(p)p^{-1}\}^r}{r}+\sum_{r=1}^{\infty}\frac{\{\chi(p)p^{-1}\}^r}{r}\right]$$

$$=\frac{1}{2}\sum_{p:素数}\left\{-\log\left(1-\frac{\chi_0(p)}{p}\right)-\log\left(1-\frac{\chi(p)}{p}\right)\right\}$$

$$=\frac{1}{2}\log\left\{\prod_{p:素数}\frac{1}{1-\frac{\chi_0(p)}{p}}\right\}+\frac{1}{2}\log\left\{\prod_{p:素数}\frac{1}{1-\frac{\chi(p)}{p}}\right\}$$

ここで $\prod_{p:素数}\frac{1}{1-\frac{\chi_0(p)}{p}}=(1-\frac{1}{3})\times\prod_{p:素数}\frac{1}{1-\frac{1}{p}}=\frac{2}{3}\times\prod_{p:素数}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$

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

$$0<\prod_{p:素数}\frac{1}{1-\frac{\chi(p)}{p}}=\prod_{p:素数}\left\{1+\frac{\chi(p)}{p}+\frac{\chi(p^2)}{p^2}+\cdots\right\}=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}$$

$$=\frac{1}{1}+\frac{-1}{2}+\frac{0}{3}+\frac{1}{4}+\frac{-1}{5}+\frac{0}{6}+\cdots$$

$$=\sum_{k=0}^{\infty}\left(\frac{1}{3k+1}-\frac{1}{3k+2}\right)<\sum_{k=0}^{\infty}\left(\frac{1}{3k+1}-\frac{1}{3k+4}\right)=1.$$

$\therefore \frac{1}{2}\log\left\{\prod_{p:素数}\frac{1}{1-\frac{\chi(p)}{p}}\right\}$ は有限値. $\therefore S=+\infty$

(I), (II) より $A+(\text{正の有限値})=+\infty$ $\therefore A=+\infty$ $\therefore \sum_{\substack{p:素数\\ p\equiv 1 \pmod 3}}\frac{1}{p}=+\infty$ //

定理5 3で割って2余る素数は無限個ある.

証明) 定理4の $Fil(n)$ にかえて

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

$Fil(0)=\frac{1}{2}(0+0)=0$, $Fil(1)=\frac{1}{2}(1-1)=0$, $Fil(2)=\frac{1}{2}(1+1)=1$

となり, 余り2の数だけ取り出せる.

あとは, 同様の計算で示せる. //

定理2,3の別証

$$\cdot\chi_0(n)=\begin{cases}0 & (n\equiv 0 \pmod 4)\\ 1 & (n\equiv 1,2,3 \pmod 4)\end{cases} \qquad \cdot\chi(n)=\begin{cases}0 & (n\equiv 0,2 \pmod 4)\\ 1 & (n\equiv 1 \pmod 4)\\ -1 & (n\equiv 3 \pmod 4)\end{cases}$$

として, $Fil_1(n)=\frac{1}{2}\{\chi_0(n)+\chi(n)\}$, $Fil_2(n)=\frac{1}{2}\{\chi_0(n)-\chi(n)\}$ とすると

Fil_1 で余り1のものだけ取り出せるし, Fil_2 で余り3のものだけ取り出せる.

あとは, $S=\sum_{r=1}^{\infty}\sum_{\substack{p:素数\\ p\equiv 1 \pmod 4}}\frac{1}{p^r}=\sum_{r=1}^{\infty}\sum_{p:素数}\frac{Fil_1(p^r)}{p^r}$ などを考える. //

定理6 一の位の数が1である素数 (11, 31, 41, 61, ‥) は無限個ある.

証明) $(\mathbb{Z}/10\mathbb{Z})^{\times}=\{1,3,7,9\}$ で $3^2\equiv 9$, $3^3\equiv 7$, $3^4\equiv 1$ より. 3で生成される巡回群で あること などから

$$\cdot\chi_0(n)=\begin{cases}0 & (n\equiv 0,2,4,5,6,8 \pmod{10})\\ 1 & (n\equiv 1,3,7,9 \pmod{10})\end{cases} \qquad \cdot\chi(n)=\begin{cases}0 & (n\equiv 0,2,4,5,6,8 \pmod{10})\\ 1 & (n\equiv 1 \pmod{10})\\ i & (n\equiv 3 \pmod{10})\\ -i & (n\equiv 7 \pmod{10})\\ -1 & (n\equiv 9 \pmod{10})\end{cases}$$

とおいて $Fil(n)=\frac{1}{4}\{\chi_0(n)+\chi(n)+\chi^2(n)+\chi^3(n)\}$ とおくと 10で割って余り1の数だけ 取り出せるということになって行き, あとは よく似た計算になる.

一般に N と d が互いに素な2つの自然数であるとき, 等差数列 (算術級数) $\{d+kN \mid k=0,1,2\cdots\}$ の中に無限個の素数があることを証明することができる. (1種だけと限らず)

それには, $(\mathbb{Z}/N\mathbb{Z})^{\times}$ の構造にもとづいて $\chi_0(n)$ や $\chi(n)$ たちを作り, そして余り d の数だけを 取り出す関数 $Fil(n)$ を作るのである.

そして, L-函数 $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ $(s>1)$ について考察すると

「$L(1,\chi_0)=+\infty$, その他の χ について $L(1,\chi)$ は有限」を示すことができ

$\sum_{\substack{p:素数\\ p\equiv d \pmod N}}\frac{1}{p}=+\infty$ が結論されるのである

(終わり)