素数とゼータ関数

砂田利一

I. 素数の話

II. ゼータ関数の誕生

参考書

[1] Paulo Ribenboim(吾郷孝視 訳):「素数の世界」，共立出版
[2] マクシミリアン・ミラー (金井省二 訳):「数学者たちのチャレンジした問題」，森北出版
[3] 上野健爾:「代数入門 1，2」(現代数学への入門)，岩波書店
[4] 砂田利一:「幾何入門 1，2」(現代数学への入門)，岩波書店
[5] 山本芳彦:「数論入門 1，2」(現代数学への入門)，岩波書店
[6] 上野健爾，砂田利一，深谷賢治，神保道夫:「現代数学の流れ I」(現代数学への入門)，岩波書店

I. 素数の話

§1.1 素数って何？

皆さん，素数って何か知っていますか？ 素数は文字通り，自然数や整数の「素」になるものです．一応，その定義を思い出しておきましょう．自然数 p が素数 (prime number) であるとは，その約数が，1 とそれ自身 p のみからなるときに言います．約数って何か知っていますね n_1 が n の約数というのは n が n_1 で割り切れるとき，すなわち $n = n_1 n_2$ となる n_2 が存在することを言います．例えば，2 と 3 は 6 の約数，2 と 7 は 14 の約数です．1 は素数の仲間には入れません．もし，n が素数でないときは，合成数とよばれます．です

から，$8=2\cdot 4$，$10=2\cdot 5$，$12=3\cdot 4$ などは合成数の例です．素数の定義は簡単ですね．でも，定義は簡単でも，素数の性質はとても複雑で，20 世紀が終わろうとしている現在でも，分からないことが多いのです．そして，今でも多くの数学者が素数に興味をもっているのです．

素数というのは，数の中でも特に自然数や整数を扱う数学の分野である「整数論」の研究対象です．そして 2500 年以上の歴史を持っているのが，素数の研究なのです．一方，この素数とは一見無関係に見える関数

$$\zeta(s)=1^{-s}+2^{-s}+3^{-s}+4^{-s}+\cdots$$

が，素数の研究に関連していることが知られています．この関数はリーマンのゼータ関数と呼ばれています．この右辺の意味は後で説明することにします．この話しの目的は，素数とゼータ関数がもつ不思議な世界に皆さんを案内することです．

§1.2 素数の性質

素数の例として，最初の幾つかを書き出しておきましょう．

$$2,3,5,7,11,13,17$$

これらが素数であることは，誰でも直ぐに確かめられます．素数の大事な性質として次の定理があります．

定理 1 素数 p が積 ab の約数ならば，p は a または b の約数である．

この事実の証明には，2 つの自然数 a，b の最大公約数を求める方法である，ユークリッドの互除法というものを使います．それを，説明するため，まず割り算の復習をしましょう．a と b が $a\geq b$ を満たす自然数であるとき，a を b で割った商が q，余りが r ということは

$$a=q\cdot b+r,\quad 0\leq r<b$$

となることを言います．このような，q と r が存在することは，次のようにして分かります．

$$0,b,2b,3b,\ldots$$

という列を考えたとき，

$$qb\leq a<(q+1)b$$

となる整数 q は必ず存在します．そして，このような q に対して

$$r=a-qb$$

と置けば，$0\leq r<b$ を満たすことが分かりますね．そして，この置き方から，$a=qb+r$ となります．こうして，商 q と余り r が定まります．余りが 0 のとき，a は b で割り切れるというのでした．

問題 1 $a = q_1 b + r_1 = q_2 b + r_2$ ， $0 \leq r_1 < b$ ， $0 \leq r_2 < b$ であるとき，$q_1 = q_2$， $r_1 = r_2$ となることを証明して下さい (言い換えれば，a， b が与えられたとき， a を b で割った商と余りは a と b により完全に決まるということです).

ユークリッドの互除法を説明しましょう．まず，実例から始めます．168 と 217 の最大公約数を求めるのに，次のような方法を用います．

$$\begin{aligned}
217 &= 1 \cdot 168 + 49 \quad (217 \text{ を } 168 \text{ で割った商が } 1, \text{ 余りが } 49) \\
168 &= 3 \cdot 49 + 21 \quad (168 \text{ を } 49 \text{ で割った商が } 3, \text{ 余りが } 21) \\
49 &= 2 \cdot 21 + 7 \quad (49 \text{ を } 21 \text{ で割った商が } 2, \text{ 余りが } 7) \\
21 &= 3 \cdot 7 \quad (21 \text{ を } 7 \text{ で割った商が } 3, \text{ 余りはなし}) \\
\Rightarrow & \quad 7 \text{ が最大公約数}
\end{aligned}$$

何故，この方法が 168 と 217 の最大公約数 7 を与えるのでしょうか．これを確かめるに，一般の自然数 a， b $(a \geq b)$ に対して今の方法を行ってみます．
a を b で割った商を q_1， 余りを r_1 とすると

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b \tag{1}$$

もし $r_1 \neq 0$ のとき，b をこの余り r_1 で割って，商を q_2， 余りを r_2 とします．

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1 \tag{2}$$

ここでも，$r_2 \neq 0$ のときには，r_1 を r_2 で割った商を q_3， 余りを r_3とします．

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2$$

$r_3 \neq 0$ のときは同じことを r_2 に対して行います．

$$r_2 = q_4 r_3 + r_4, \quad 0 \leq r_4 < r_3$$

これを続けていくと，

$$r_1 > r_2 > r_3 > r_4 > \cdots (\geq 0)$$

となりますから， いつかは $r_n = 0$ となります．すなわち，余りがなくなるときが必ずあるはずです．

このような n に対して， 最後の 2 つの式を書いておきましょう．

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2} \tag{3}$$

$$r_{n-2} = q_n r_{n-1} \tag{4}$$

さて，ここで r_{n-1} に注目します．これが a， b の最大公約数であることを証明しましょう．

最後の式 (4) から，r_{n-2} は r_{n-1} で割り切れます．よって，直前の式 (4) から r_{n-3} も r_{n-1}で割り切れますね．さらにその前の式を使うと r_{n-4} も r_{n-1}で割り切れることが分かります．これを前へ前へと続けていけば，r_{n-1}はすべての r_i $(i = 1, 2, \ldots, n-2)$ を割り切

りますから，最初の 2 つの式 (1)，(2) から，a と b を割り切ることになるのです．従って，r は a，b の公約数になります．

逆に，r が a，b の公約数とすると，今度は最初の 2 つの式から始めて，下に順に見て行くと，r_{n-1} が r で割り切れることが分かりますね．と言うことは，r_{n-1} は a，b の任意の公約数の倍数ということであり，結局 r_{n-1} は a，b の最大公約数となるのです．

問題 2 76084 と 63020 の最大公約数を求めよ．

a，b の最大公約数が 1 であるとき，a，b は互いに素であるといいます．さて，定理 1 の証明を行うため，まず次の一般的定理を証明します．

定理 2 積 ac が b で割り切れ，しかも，a と b が互いに素であるとき，c が b で割り切れる．

証明 ユークリッドの互除法を適用します．a と b の最大公約数は 1 ですから，$r = 1$ となっています．

$$
\begin{aligned}
a &= q_1 b + r_1 && (5)\\
b &= q_2 r_1 + r_2 && (6)\\
r_1 &= q_3 r_2 + r_3, && (7)\\
&\cdots \quad \cdots \quad \cdots &&\\
r_{n-3} &= q_{n-1} r_{n-2} + 1 && (8)
\end{aligned}
$$

これらの式の両辺に c を掛けます．

$$
\begin{aligned}
ac &= q_1 bc + r_1 c && (9)\\
bc &= q_2 r_1 c + r_2 c && (10)\\
r_1 c &= q_3 r_2 c + r_3 c && (11)\\
&\cdots \quad \cdots \quad \cdots &&\\
r_{n-3} c &= q_{n-1} r_{n-2} c + c && (12)
\end{aligned}
$$

仮定により，ac は b で割り切れますから，(9) から $r_1 c$ が b で割り切れることになります．(10) を見ると，bc，$r_1 c$ の両方が b で割り切れますから，$r_2 c$ が b で割り切れることになります．同様に (11) から $r_3 c$ が b で割り切れることになります．これを続けて行けば，最後の式まで達することになり，$r_{n-3} c$ と $r_{n-2} c$ が b で割り切れることが分かりますから，結局 c が b により割り切れることが証明されました．

最初の定理に戻りましょう．仮定では，積 ab が p で割る切れるということでした．もし，p が a の約数であれば，言っていることは正しいですから，p が a の約数でないとします．a と p の最大公約数はもちろん 1 です．従って，定理 2 から，b が p で割り切れるのです (定理 1 の証明終わり)．

問題 3 a と b が互いに素で，a，b がそれぞれ c の約数であるとき，積 ab も c の約数であることを示して下さい．

何故，素数が自然数や整数の「素」なものとかというと，すべての自然数はいくつかの素数の積として表されるからです．例えば，

$$\begin{aligned} 4 &= 2\cdot 2 = 2^2, \quad 6 = 2\cdot 3, \quad 8 = 2\cdot 2\cdot 2 = 2^3, \\ 9 &= 3\cdot 3 = 3^2, \quad 10 = 2\cdot 5, \quad 12 = 2\cdot 2\cdot 3 = 2^2\cdot 3, \\ 14 &= 2\cdot 7, \quad 15 = 3\cdot 5, \ldots, 24 = 2\cdot 2\cdot 2\cdot 3 = 2^3\cdot 3, \ldots, \\ 120 &= 2\cdot 2\cdot 2\cdot 3\cdot 5 = 2^3\cdot 3\cdot 5 \end{aligned}$$

「素」なものというと，素粒子を思い浮かべる人もいると思います．どんな物質も素粒子が集まってできていて，素粒子はそれ以上に分解できない物質ですから，丁度素数と同じ感じですね (最近の研究では，さらにクウォークと呼ばれる粒子に分解されるそうですから，言い方を変えなければなりませんが，いずれにしても物理学では，最小単位の粒子が存在するという確信があるようです)．上で述べたことを一般の形で述べたのが次の**素因数分解定理**です．

定理 3 n を任意の自然数とするとき，n は

$$n = q_1 q_2 \cdots q_h, \quad q_1 \leq q_2 \leq \cdots \leq q_h$$

のように，素数の積としてただ一通りに表すことができる．

別の表し方をすると，現れる素数の中で同じものをまとめることにより

$$n = p_1^{k_1} \cdots p_m^{k_m}; \quad p_1 \ldots, p_2 \text{ は互いに異なる素数}$$

となります．

念のため証明を与えておきましょう．おおげさかも知れませんが n に関する帰納法を使います．

(1)　もし n が 1，n と異なる約数を持たなければ，n 自身が素数．

(2)　$n = n_1 n_2$，$n_1 < n$，$n_2 < n$ とすれば，帰納法の仮定により，n_1，n_2 は素数の積で表されるから，n も素数の積で表される．それを小さい方から順に並べ換えればよい．

(証明終わり)

素因数分解の一意性を言うために

$$n = q_1 q_2 \cdots q_h = q_1' q_2' \cdots q_k', \tag{13}$$

を 2 つの素因数分解とします．定理 1 で述べたことから q_1 は

$$q_1', q_2', \ldots, q_k'$$

のどれかを割り切りますから，例えばそれを q_i' とすると $q_1 = q_i'$ でなければなりません．(13) から q_1 と q_i' を除いたものはもちろん等式ですから，同様に，$q_2 = q_j'$ となる q_j' $(I \neq j)$ が存在します．これを続ければ，$h = k$ かつ q_1'，$q_2', \ldots, q_k'$ は q_1，$q_2, \ldots, q_h$ を並べ換えたものになることがわかります．

(証明終わり)

問題 4 120 と 999999 の素因数分解を求めて下さい.

§1.3 素数の表の作り方

上で 10 より小さい素数を与えましたが，ついでだから，100 より小さい素数も全部書き出しておきましょう.

$$11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

これも，1 つ 1 つ確かめることで，100 以下の素数はこれらがすべてであることが確かめられます. こうしてみると，直ぐに分かることは，2 を除いて素数はすべて奇数であることです. 実際，2 の倍数である偶数は，2 を除いて素数にならないことは，素数の定義から直ぐに分かりますね. 奇数がすべて素数でないことは，例えば，9 がその例となっていることから分かります.

では，上に上げた素数の表を続けていくにはどうすればよいでしょうか. 100 から始めて，一つ一つの数の約数を調べることも 1 つの方法です. でも大きな数になると大変ですね. 例えば，30031 は素数でしょうか. そんなに簡単ではないでしょう (答えは後で言います). もっと，系統立った方法で，素数の表を作る方法はないのでしょうか. それがあるのです. それはエラトステネス (紀元前 276–194) が考えた方法で，次のように行うのです. まず，小さい方から順に並べた自然数の表を用意します.

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$$

まず，1 は素数ではありませんから，斜線を引いて除きます. 次ぎに 2 は素数ですからそのままにしておいて，2 の倍数となる自然数，すなわち 2 以外の偶数に斜線を引いて除きます. すると除いたもの中で 3 が最初の数ですね. 今度は，この 3 の倍数 (3 以外) を斜線を引いて除きます. 残った数の最初の数は 5 ですから，同じように 5 の倍数 (5 以外) を斜線を引いて除きます. この後の操作は誰でも分かりますね. これを続けて残った数が素数全体になるのです. どうしてか考えてみて下さい. 今述べた方法を，**エラトステネスの篩 (ふるい)** と言います.

ところで，エラトステネスは，地理学者としても偉大な人でした. 例えば，2 つの地点で太陽が差し込む角度を使って地球の子午線の長さを測ったことでも知られています (彼の計算は，現在知られている実際の子午線の長さと 16% しか違いませんでした!).

問題 5 n が合成数であれば，n は 1 と異なる n 以下の約数をもつことを証明して下さい. これは，与えられた自然数 n が合成数かどうか調べるのに，n 以下の数で n が割り切れるかどうかを確かめればよいことを意味しています. (ヒント $n = n_1 n_2$, $1 < n_1 \leq n_2 < n$ と表されますから $n_1^2 \leq n_1 n_2 = n$)

問題 6 100 までの素数表を自分で作ってください.

§1.4 素数は幾つある？

さて，素数表を作ることはできましたが，ここで次のような疑問が浮かびます．素数は限りなく存在するのでしょうか．このような疑問は，素数の表を見ていると自然に沸き起こります．しかし，エラトステネスの篩では，素数が無限個存在するかどうかには答えられません．もしかしたら，素数の表は有限のところで途切れてしまうかもしれません．ここで，再び有名なユークリッドに登場してもらわなければなりません．

ユークリッドの名前は聞いたことがあるでしょう．中学・高校で学ぶ幾何学は，古代ギリシャ時代に，ターレス，ピタゴラス，ユードクソスなどの数学者が作り上げたものですが，ユークリッドはそれまで知られていた結果を「原本」として纏めました.「原本」では，まず公理という，前提となる仮定をおいて，論証により議論を進めていく方法をとっています．例えば

「直線と，その上にはない点が与えられたとき，この点を通り，直線と交わらない (平行な) 直線はただ 1 つ存在する」

というのは，表現こそこれとは違いますが，ユークリッドが公理の 1 つとして仮定したものです．この公理のお陰で「三角形の内角の和は 180 度」という定理が証明されるのです．いずれにしても，そのユニークな書き方は，時代を超越するものでした．実際，後代になって，科学者のニュートンや哲学者のスピノザは，ユークリッドの書き方に倣っています．20 世紀の中頃に始まったブルバキという数学者集団が書いた「数学原論」という壮大なシリーズも，ある意味でユークリッドの「原本」をお手本にしているのです (参考書 [4])．

素数の話に戻りましょう．ユークリッドの「原本」には定理として，次のことが述べられています．

「素数は無限個存在する」

ユークリッドの証明を紹介しましょう．それは，背理法によるものです．すなわち，素数が有限個しか存在しないとすると矛盾が生じることを言うのです．$2, 3, 5, \ldots,$ p を素数のすべてとしましょう．これらの積を考えて，それに 1 を足します:

$$N = 2 \cdot 3 \cdot 5 \cdot p + 1$$

この数の性質を見ましょう．まず，どんな素数で割っても 1 が余りますね．ということは，N 自身素数ということにはならないでしょうか．もし，N が素数でなければ，素因数分解定理により N は N より小さい素数で割り切れるはずですから，今言ったことに反しますから，N は素数です．ところが N は最大の素数 p より大きい数ですから，これは矛盾です．だから最大の素数は存在しないことになって，素数は無限個存在することになるのです．

この証明を見て，次のような問題を考えることができます．

(1)　$N_p = 2 \cdot 3 \cdot 5 \cdots p + 1$ が素数となるような素数 p は無限にあるか

(2)　$N_p = 2 \cdot 3 \cdot 5 \cdots p + 1$ が合成数となるような素数 p は無限個あるか．

答えは，今のところ知られていません．

例　$p = 11$ のとき，$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ は素数

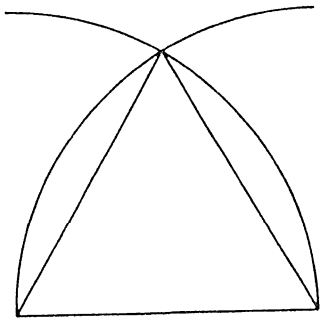
$p = 13$ のとき $N = 30031 = 59 \cdot 509$

(ある数学の啓蒙書では，すべての N が素数と言っていますが，これは間違いです).

§1.5 素数と幾何学

ここで，何故，数学者が素数に興味を持つのか，説明してみましょう．それは，素数が見かけによらず，色々なことに関係しているからです．例えば，正多角形の作図問題がその1つです．

定規とコンパスで色々な図形を作図する問題のことをご存じだと思います．例えば，与えられた辺をもつ正三角形の作図は次のように行いますね．



正方形，正5角形も作図できます．18世紀までは，作図のできる正多角形は，n を辺の数とするとき，$n = 3, 4, 5$ の正多角形と，もっと一般にはその辺の数が $n = 3, 4, 5$ の1つと2のベキの積

$$
\begin{aligned}
n &= 3, 6, 12, 24, 48, \ldots (= 3 \cdot 2^k; k = 0, 1, 2, \ldots) \\
n &= 4, 8, 16, 32, 64, \ldots (= 4 \cdot 2^k; k = 0, 1, 2, \ldots) \\
n &= 5, 10, 20, 40, 80, \ldots (= 5 \cdot 2^k; k = 0, 1, 2, \ldots)
\end{aligned}
$$

および，3×5 と2のベキの積

$$n = 15, 30, 60, 120, \ldots (= 2^k \cdot 3 \cdot 5; k = 0, 1, 2, \ldots)$$

の場合しか知られていませんでした．そして，これ以外の正多角形の作図など，誰も可能だとは思っていなかったのです．

丁度200年前の1796年の3月30日のことでしたが，19歳の青年ガウスは，ベッドからまさに起きようとするときに，正17角形の作図を思いついたのです．ガウスが数学者になろうと決心したのは，まさにこのときであったと伝えられています．

さらにもっと一般に，ガウスは，辺の数が $n = 2^{2^k} + 1$ の形の素数であるとき，それが作図可能であることを示しました．いくつかの例で確かめてみましょう．

$$
\begin{aligned}
3 &= 2 + 1 \\
5 &= 2^2 + 1 \\
17 &= 2^4 + 1 \quad \text{(これがガウスの扱った場合です)}
\end{aligned}
$$

$$257 = 2^8+1$$
$$65537 = 2^{16}+1$$

はすべて素数です.

$2^{2^k}+1$ の形の数をフェルマー数といいます. なぜフェルマー数というのかと言うと, フェルマーは, このような数はすべて素数と信じて, 証明を与えようとした経緯があるからです. ところが $2^{32}+1$ $(32=2^5)$ は素数ではありません (10 桁の数です). 実際, これは 641×6700417 と素因数分解されます (オイラー).

一般に, 大きい数が素数であるかどうかを判定することは用意ではありません. ましてや, 素数ないときに, その素因数を見つけることはとても手間の掛かることなのです (最近では, このようなことから, 大きな数の素因数分解を暗号に使うことが行われています). オイラーも, $2^{32}+1$ の素因数分解を行うのに, 特別な判定法を開発して, それを応用したのです. なぜ, このような数が, 正多角形の作図の問題と関係があるのでしょうか. それは, 方程式

$$x^n-1=0 \tag{14}$$

の根が, 幾つかの平方根を組み合わせて解くことができることに対応しているのです (ただし, 複素数が現れます). 例えば, $x^3-1=0$ は

$$(x-1)(x^2+x+1)=0$$

となりますから, これから

$$x=1,\quad \frac{-1\pm\sqrt{3}i}{2}$$

となります. ここで i は虚数単位を表します.

問題 7 正 5 角形に対する円周等分方程式

$$x^5-1=0$$

が, 平方根のみを使って解けることを示して下さい

ガウスの発見は, 最近のフェルマー予想の解決に繋がる現代整数論の始まりを告げるものでもあったのです. (フェルマー予想については, 黒川先生から詳しいお話しがあると思います.)

問題 8 2^n+1 が素数であれば, $n=2^k$ となることを示して下さい. (ヒント: n を素因数分解したとき, もし奇素数が現れたとします. $n=ab$ (b は奇数) と書けますから,

$$2^n+1=(2^a)^b+1$$

と表されます. ここで, 一般に x^b+1 についての因数分解

$$x^b+1=(x+1)(x^{b-1}-x^{b-2}+x^{b-3}-\ldots+1)$$

が成り立つことに注意して下さい. b が偶数であるときは, このような因数分解は持ちません.)

II ゼータ関数の誕生

§2.1 調和級数とオイラーの証明

ユークリッドの証明は，文句のつけようのないものです．でも，素数の分布をもっと詳しくしるには，ほとんど役には立ちません．素数が無限個存在することの証明は他にも知られていますが，中でも有名なものはオイラーによるものです．そして，この証明が素数の研究をさらに進める出発点となったのです．これを説明するため，まず次のような和を考えましょう．

$$1+2^{-1}+3^{-1}+\ldots+n^{-1}$$

そして，n を大きくしていきます．すると，この和もどんどん大きくなって，無限大になることが次のようにして分かります．

$$\begin{aligned}
1 \;+\; & 2^{-1}+3^{-1}+4^{-1}+5^{-1}+6^{-1}+7^{-1}+8^{-1} \\
& +9^{-1}+10^{-1}+11^{-1}+12^{-1}+13^{-1}+14^{-1}+15^{-1}+16^{-1}+\ldots \\
> 1 & +2^{-1}+\underbrace{4^{-1}+4^{-1}}_{2}+\underbrace{8^{-1}+8^{-1}+8^{-1}+8^{-1}}_{4} \\
& +\underbrace{16^{-1}+16^{-1}+16^{-1}+16^{-1}+16^{-1}+16^{-1}+16^{-1}+16^{-1}}_{8}+\ldots \\
= 1 & +2^{-1}+2^{-1}+2^{-1}+2^{-1}+\ldots \\
= \quad & \infty
\end{aligned}$$

すなわち，

$$1+2^{-1}+3^{-1}+\ldots+n^{-1}+\ldots=\infty$$

ということになります．これを「調和級数は発散する」と言います．

このことと，素数が無限個存在することとはどう結び付くのでしょうか．ここで，等比級数のことを思い出しましょう．

$$1+r+r^2+\ldots+r^{n-1}=\frac{1-r^n}{1-r}$$

という公式は知っていると思います．ここで，r が 1 より小さい正の数とすると r は n を大きくするときいくらでも 0 に近づきますから

$$1+r+r^2+\ldots+r^n$$

は $(1-r)^{-1}$ に近づいていきますね．このことを

$$1+r+r^2+\ldots=(1-r)^{-1}$$

と書くことにしましょう．ここで，r として，素数 p の逆数 p^{-1} を取ります．すると

$$1+p^{-1}+p^{-2}+\ldots=(1-p^{-1})^{-1}$$

となりますね．q も素数として同じことを行うと

$$1+q^{-1}+q^{-2}+\cdots=(1-q^{-1})^{-1}$$

さて，ここで積

$$(1+p^{-1}+p^{-2}+\cdots)(1+q^{-1}+q^{-2}+\cdots)$$

を考えて，これを展開してみましょう．無限和の展開なんて考えたこともないという人がいると思いますが，そんなに恐れる必要はありません．

$$\begin{aligned}
1 \quad \times \quad & (1+q^{-1}+q^{-2}+\cdots) \\
& +p^{-1}\times(1+q^{-1}+q^{-2}+\cdots) \\
& +p^{-2}\times(1+q^{-1}+q^{-2}+\cdots) \\
& +\cdots \\
= \quad & (1+q^{-1}+q^{-2}+\cdots)+(p^{-1}+p^{-1}q^{-1}+p^{-1}q^{-2}+\cdots) \\
& +(p^{-2}+p^{-2}q^{-1}+p^{-2}q^{-2}+\cdots) \\
& \cdots \\
= \quad & (p^aq^b) \text{ において } a,\ b \text{ をすべての自然数および } 0 \text{ として動かしたときの和．}
\end{aligned}$$

この考え方を使って，$p_1,\ p_2,\ldots,p_k$ を異なる素数としたとき

$$1-p_1^{-1})^{-1}(1-p_2^{-1})^{-1}\cdots(1-p_k^{-1})^{-1} \tag{15}$$

を展開すると，

$$(p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k})^{-1}$$

の形の項を持つ和となることが分かります．ただし，和は $e_1,\ e_2,\ldots,e_k$ をすべての自然数と 0 を動かして得られるものです．ここで，素数が有限個しか存在しないとして，それを $p_1,\ p_2,\ldots,p_k$ としましょう．すると，任意の自然数 n は

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

と一意的に表されることを素因数分解定理のところで述べました．ということは，上で考えた積 (15) は

$$n^{-1}$$

の形を持つ項を持つ和に等しいことになります．ここで，n はすべての自然数を動くのですから，これは調和級数

$$1+2^{-1}+3^{-1}+\cdots$$

に等しいので，前に示したように値は無限大です．すなわち，

$$(1-p_1^{-1})^{-1}(1-p_2^{-1})^{-1}\cdots(1-p_k^{-1})^{-1}=\infty$$

という奇妙な式が得られることになります．左辺は有限の値なのに，これは矛盾ですね．こうして，素数が無限個あることになるのです．

ここで，指数関数について説明しましょう．a を 1 と異なる正数とします．n を自然数とするとき，a の n 乗 a^n は a を n 個掛け合わせたものです．

$$\begin{aligned} a^m a^n &= a^{m+n} \\ (a^m)^n &= a^{mn} \end{aligned}$$

という式は皆さん知っているはずです．約束として，$a^0 = 1$，$a^{-n} = (a^n)^{-1}$ と定義すると，これらの式は，すべての整数 m，n に対して成り立つことも習いました．a の有理数乗を定義するため，まず

$$a^{1/q}$$

は a の q 乗根とします．すなわち，$b^q = a$ となる正数 b を $a^{1/q}$ と置くのです．有理数 p/q に対して，

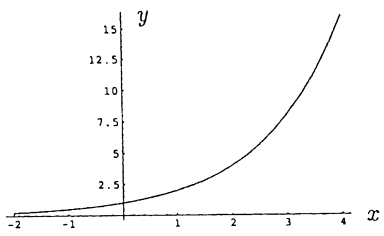
$$a^{p/q} = (a^p)^{1/q}$$

とおいて，a の有理数乗を定義します．すると r，s を任意の有理数とするとき

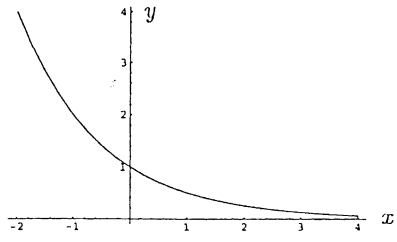
$$\begin{aligned} a^r a^s &= a^{r+s} \\ (a^r)^s &= a^{rs} \end{aligned}$$

となることが確かめられます．

a の実数乗は，極限の考え方を用いて定義されます．x を実数としたとき，x に近づく有理数の列 r_1，$r_2, \ldots, r_n, \ldots$ を考え，n を大きくしていったときに，a^{r_n} が近づく値を a^x とするのです．この a^x も上の性質をそのまま満たすことが分かります．こうして，各 x に $y = a^x$ を対応させることにより，x の関数が得られますが，これが (a を底とする) 指数関数とよばれるものです．指数関数のグラフは次のような形をしています．



(a＞1)



(a＜1)

この指数関数を使えば，実数 s に対して n^{-s} を考えることができます．そして，和

$$1 + 2^{-s} + 3^{-s} + \cdots + n^{-s}$$

を考察してみましょう．

ちょっと不思議に思うかも知れませんが，s を 1 より少しでも大きい数とすると

$$1 + 2^{-s} + 3^{-s} + \cdots + n^{-s}$$

は n を大きくしても有限の値に近づくことが分かります．例えば，$s=2$ とすると，この値は $\pi^2/6$ となることがオイラーにより証明されました．

$$\zeta(s) = 1 + 2^{-s} + 3^{-s} + \cdots + n^{-s} + \cdots$$

と書いて，これをリーマンのゼータ関数といいます．前に述べたことから，

$$\zeta(s) = (1-2^{-s})^{-1}(1-3^{-s})^{-1}\cdots(1-p^{-s})^{-1}\cdots$$

と表されることは容易に理解できますね．これをゼータ関数のオイラー積表示といいます．この関数がもつ不思議さは，現在でも解けない問題として残っているのです．

§2.2 素数の密度

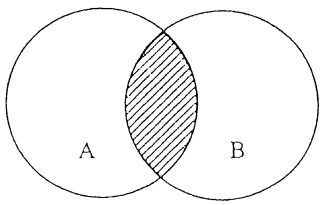
さて，素数が無限個あると分かりましたから，今度は，自然数と較べて，どの位あるのかを調べましょう．もちろん，自然数よりは「少ない」ということは確かです．ここで「少ない」という言い方をしました．もし，2つの「もの」の集まりが共に有限個の「もの」からなっているのなら,「もの」の多さを比較できます．でも，自然数の全体は無限ですし，素数も無限個あるのです．無限個のものを比較するにはどうすればよいのでしょうか．偶数の全体を考えます．もちろん偶数も無限個ありますね．自然数と較べて，偶数はどのくらいあるか考えるのです．アバウトな言い方では，何となく，偶数の多さは自然数に較べて丁度半分と思えませんか．これをちゃんと言うにはどうすればよいでしょうか．ここで，密度という考え方が生まれます．密度というと，物質の密度を思い出します．物体の単位容積に含まれている質量が密度というものです．これから説明する密度も，これと似た感じのものです．

ここで，ちょっと記号を導入します．

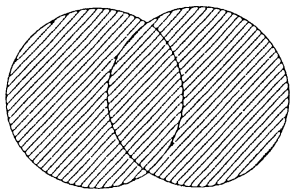
皆さん，集合と言う言葉を知っていますか．集合とは,「もの」の集まりのことです．例えば，自然数の全体や，素数の全体は集合です．数学者は，一般の集合を表すのに，大文字のアルファベットを使います．例えば，A，B，S などがそうです．自然数の全体からなる集合を $\mathbf{N}$ により表しましょう．また，素数の全体は，$\mathbf{P}$ により表すことにします．2つの集合 A，B に対して，A にも B にも属する「もの」全体からなる集合を A と B の共通部分といい，$A\cap B$ により表します．また，A または B に属する「もの」全体からなる集合は A と B の和といい，$A\cup B$ により表します．もっと，一般に，3つ以上の集合 A，B，C,... に対しても，共通部分と和を同様に定義します．そして，それらを

$$A\cap B\cap C\cap\cdots$$
$$A\cup B\cup C\cup\cdots$$

と表します．



A∩B



A∪B

集合 B が A の一部分であるとき，$B \subset A$ と書くことにします．そして，B を A の部分集合といいます．ここで特に扱うのは，自然数の集合 $\mathbf{N}$ の部分集合です．2 つの集合 A，B に対して，差 $A - B$ は，A に属し，B には属さない「もの」からなる集合を表します．

問題 9 集合 A, B, C に対して

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

を証明して下さい．

集合 A が有限個の「もの」から成っているとき，A を有限集合といい，その「もの」の個数を $\#A$ と書くことにしましょう．例えば，

$A = \{2, 4, 6\}$ のとき $\#A = 3$

$A = \{2, 3, 5, 7, 11, 13\}$ のとき $\#A = 6$

となります．次の基本的公式は，後で大変有用です．A, B, C がすべて有限集合であるとき

$$\begin{aligned} \#(A \cup B) &= \#A + \#B - \#(A \cap B) \\ \#(A \cup B \cup C) &= \#A + \#B + \#C - \#(A \cap B) - \#(B \cap C) \\ &\quad - \#(C \cap A) \quad + \#(A \cap B \cap C). \end{aligned}$$

最初の式は，A と B の共通部分がなければ明らかです．このときは，

$$\#(A \cup B) = \#A + \#B$$

となるからです．一般の場合には，$(A - (A \cap B)) \cup B = A \cup B$ であり，$A - (A \cap B)$ と B は共通部分を持ちませんから，

$$\begin{aligned} \#(A \cup B) &= \#(A - (A \cap B)) + \#B \\ &= \#A - \#(A \cap B) + \#B \end{aligned}$$

となりますから，求める式が得られました．

2 番目の式はどうでしょうか．$A \cup B \cup C$ は $(A \cup B) \cup C$ と同じ集合ですから，最初の式を適用して

$$\begin{aligned} \#((A \cup B) \cup C) &= \#(A \cup B) + \#C - \#((A \cup B) \cap C)) \\ &= \#A + \#B - \#(A \cap B) - \#((A \cap C) \cup (B \cap C)) \\ &= \#A + \#B - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) \\ &\quad + \#((A \cap C) \cap (B \cap C)) \\ &= \#A + \#B + \#C - \#(A \cap B) - \#(B \cap C) - \#(C \cap A) \\ &\quad + \#(A \cap B \cap C) \end{aligned}$$

となります．

問題 10 上の式を，4 つの有限集合 A, B, C, D の場合に拡張して下さい．さらに，n 個の有限集合に対しては，どのような式が期待できますか？できれば，その証明も与えて下さい．

自然数 k に対して，k の倍数となるもの全体を $A(k)$ と書きましょう．すなわち

$$A(k) = \{k, 2k, 3k, 4k, \ldots\}$$

です．$A(k)$ は $\mathbf{N}$ の部分集合です．

自然数 h と k の最大公約数が 1 のとき，h，k は**互いに素**であると言います．このとき，$A(h)$ と $A(k)$ の共通部分はどうなるでしょうか．$A(h) \cap A(k)$ に属する数は，h の倍数でもあり，同時に k の倍数でもある数です．すると，h，k は互いに素ですから，そのような数は hk の倍数でなければなりません．従って答えは $A(hk)$ です：

$$A(h) \cap A(k) = A(hk).$$

3 つ以上の自然数 $h, k, \ell, \ldots$ に対して，どの 2 つも互いに素とするとき，

$$A(h) \cap A(k) \cap A(\ell) \cap \cdots = A(hk\ell \cdots)$$

となることも分かります．$\mathbf{N}$ の部分集合 A の密度を定義するため，各自然数 n に対して，共通部分

$$A_n = A \cap \{1, 2, 3, \ldots, n\}$$

を考えましょう．すなわち，A に属する数で，n 以下のもの全体です．そして，商

$$\#A_n/n$$

を考えます．ここで $\#A_n$ は A_n に属する数の個数を表していることを思い出して下さい．これは $\{1, 2, \cdots, n\}$ に属する A の数の割合を表しています．もちろん，この割合は 1 以下の数ですね．

この商において，n をどんどん大きくしたとき，ある数に近づけば，この数を A の密度ということにします．そして，これを $D(A)$ と書くことにします．

$$0 \leq D(A) \leq 1$$

となることは容易に理解できますね．

注意　$\mathbf{N}$ の部分集合すべてが密度をもつわけではありません．しかし，この話で扱う部分集合は密度をもつ集合です．もし，このような場合でも，大きい n に対して $\#A_n/n$ が c 以下のとき，密度は高々 c であるといいます．

さて，$A(k)$ の密度はいくつでしょうか．答えは $1/k$ です．これは，直観的には明らかですが，数学的証明は次のように行います．

自然数 n を k で割った商を q，余りを r としましょう：

$$n = qk + r, \quad 0 \leq r < k \tag{16}$$

このとき，このとき，$A(k)\cap\{1,2,\ldots,n\}$ に属する数の個数はいくつありますか．$mk\leq n$ となる最大の m がその個数ですね．このことから，この最大の m は q と等しいことが分かります (実際，$qk\leq n<(q+1)k$)．よって

$$\#(A(k)\cap\{1,2,\cdots,n\})/n=q/n$$

となります．

(16) を眺めてみましょう．両辺を nk で割ると

$$1/k=q/n+r/nk$$

ですね．ここで，n を大きくすると，$r/nk\leq 1/n$ ですから，左辺の第 2 項は 0 に近づいていきます．

こうして，q/n は n を大きくすると $1/k$ に近づくのです．故に，$A(k)$ の密度は $1/k$ に等しいことが分かりました．

さて，h,k が互いに素であるとき

$$A(h)\cap A(k)=A(hk)$$

でした．よって

$$D(A(h)\cap A(k))=D(A(hk))=1/hk=(1/h)\cdot(1/k)=D(A(h))D(A(k))$$

となります (もし，確率のことを学んでいれば，この等式は，事象の独立性を表す式と似ていることに気づくと思います)．

ここで，$\mathbf{N}$ の一 般の部分集合 A の場合に戻ります．$\mathbf{N}$ から A を除いたものを A^c と書きましょう．例えば，$A(2)^c$ は奇数の集合です．一 般に $A(k)^c$ は k で割り切れない数の全体です．

$$(A\cap B)^c=A^c\cup B^c$$

であることは簡単に分かります．

A が密度 $D(A)$ を持つとき，A^c の密度はいくつになるでしょうか．答えは $1-D(A)$ になります：$D(A^c)=1-D(A)$．証明は簡単です．

$$\#(A^c\cap\{1,2,\cdots,n\})=n-\#(A\cap\{1,2,\cdots,n\})$$

を使えばよいのです．

次の等式はどうでしょうか．$A,B,A\cap B$ が密度を持っとき，$A\cup B$ も密度を持ち

$$D(A\cup B)=D(A)+D(B)-D(A\cap B).$$

証明には，次の式を使います：

$$\begin{aligned}\#((A\cup B)\cap\{1,2,\ldots,n\}) &= \#(A\cap\{1,2,\ldots,n\})+\#(B\cap\{1,2,\ldots,n\})\\ &\quad -\#((A\cap B)\cap\{1,2,\ldots,n\})\end{aligned}$$

問題 11 $A, B, C, A\cap B, \cap C, C\cap A, A\cap B\cap C$ が密度を持っとき，

$$\begin{aligned} D(A\cup B\cup C) &= D(A)+D(B)+D(C)-D(A\cap B) \\ &\quad -D(B\cap C)-D(C\cap A)+D(A\cap B\cap C) \end{aligned}$$

であることを示して下さい．

密度の公式を使えば，次の定理が得られます．

定理 4 $D(A\cap B)=D(A)D(B)$ であるとき，

$$D(A^c\cap B^c)=D(A^c)D(B^c)$$

証明

$$\begin{aligned} D(A^c\cap B^c) &= D((A\cup B)^c)=1-D(A\cup B)=1-\{D(A)+D(B)-D(A\cap B)\} \\ &= 1-D(A)-D(B)+D(A)D(B) \\ &= (1-D(A))(1-D(B)) \\ &= D(A^c)D(B^c) \quad (\text{証明終わり}) \end{aligned}$$

この定理を，$A=A(h)$，$B=B(k)$ に適用してみましょう（h, k は互いに素）．

$$D(A(h)^c\cup A(k)^c)=D(A(h)^c)D(A(k)^c)=(1-1/h)(1-1/k)$$

となりますね．ここで $A(h)^c\cap A(k)^c$ は，h でも k でも割り切れない数の全体であることに注意して下さい．

問題 12 h, k, ℓ のどの 2 つも互いに素であるとき，

$$D(A(h)^c\cap A(k)^c\cap A(\ell)^c)=(1-1/h)(1-1/k)(1-1/\ell)$$

となることを示して下さい．

今までは，2 つの素な数で考えてきましたが，3 つ以上の数 $h, k, \ell, \cdots$ に対しても，そのうちのどの 2 つの素な場合には，$h, k, \ell, \cdots$ のどの数でも割り切れない数の全体のなす集合 A は，密度

$$(1-1/h)(1-1/k)(1-1/\ell)\cdots$$

を持つことが分かります．ここで，$h, k, \ell, \cdots$ として，素数 $2, 3, \cdots, p$ を考えましょう．$2, 3, \cdots, p$ のどれでも割り切れない数，すなわち，素因数分解に $2, 3, \cdots, p$ が現れない数の集合の密度は

$$(1-1/2)(1-l/3)\cdots(1-1/p)$$

となることが分かりました．

さて，p より大きい素数の集合は，もちろん素因数分解に $2, 3, \cdots, p$ が現れない数の集合に含まれます．ですから，その密度は高々

$$(1-1/2)(1-1/3)\cdots(1-1/p)$$

であることが分かりますね.

ところで, 一般に $\mathbf{N}$ の部分集合 A に有限個の数からなる部分集合を合わせても, その密度は A の密度と変わりません. ですから, 結局素数の集合 $\mathbf{P}$ の密度は $(1-1/2)(1-1/3)\cdots(1-1/p)$ より小さいことが分かります.

さて $(1-1/2)(1-1/3)\cdots(1-1/p)$ において, 素数 p を大きくとっていくとどうなるでしょうか. 前に見たように, この逆数は調和級数に近づいていきますから, それは無限大に近づきます. 従って, $(1-1/2)(1-1/3)\cdots(1-1/p)$ は 0 に近づくきます.

こうして, 素数の集合 $\mathbf{P}$ の密度は, どんな小さい数より小さくなり, 結局 0 に等しいことが分かります. 無限個あるのに密度が 0 になるのは, 素数が疎らにしか現れないことを意味しているのです. この節の締めくくりに, 連続する素数の間にある合成数の個数が幾らでも大きくできることを示しましょう.

N を任意の自然数とします. そして

$$(N+1)!+2, (N+1)!+3, \ldots, (N+1)!+N+1$$

を考えます. ここで一般に, $n!$ は n の階乗 $n!=n(n-1)(n-2)\cdots3\cdot2\cdot1$ を表します. 上の列に現れる数が, すべて合成数であることは明らかですから, N 個の連続した合成数が存在することになるわけです.

§2.3 素数分布

さて, 素数の密度は 0 となることは分かりましたが, 素数の分布のもっと詳しい情報を得ることはできないのでしょうか. この問題を考えるため, 簡単な例を見てみましょう. 平方数の列

$$A=\{1^2, 2^2, 3^2, \ldots\}$$

を考えます. まず, この密度はどうなるでしょうか. $i^2 \leq n$ とすると, $i \leq \sqrt{n}$ ですから, n 以下の平方数の個数は $\sqrt{n}$ 以下です. よって,

$$\#A_n/n \leq \sqrt{n}/n$$

となって, これは零に近づいていきます. ですから, 平方数の密度は 0 になります. ここで, $(\sqrt{n})-1 \leq \#A_n \leq \sqrt{n}$ を使えば, n を大きくしていったとき,

$$\frac{\#A}{\sqrt{n}} \to 1$$

となることが分かります. 言い換えれば, $\#A$ は $\sqrt{n}$ と同じ程度の大きさを持っていると言って差し支えないでしょう.

一般に, $\mathbf{N}$ の部分集合 A に対して, 関数 $f(n)$ が存在して,

$$\frac{\#A}{f(n)} \to 1 \quad (n \to \infty)$$

が成り立つとき

$$\#A \sim f(n)$$

と書くことにします．A が平方数の集合の場合は，上でみたことから

$$\#A \sim \sqrt{n}$$

と表されるわけです．

さて，素数の集合 $\mathbf{P}$ の場合に，何か簡単な関数 $f(n)$ により

$$\#\mathbf{P}_n \sim f(n)$$

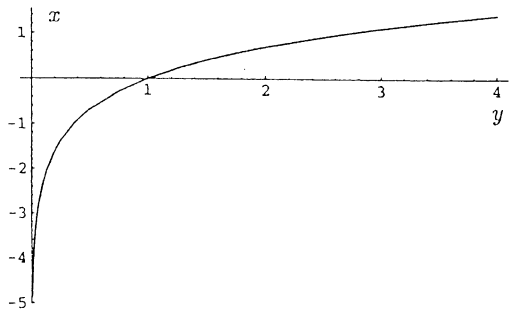
と書けるでしょうか．

この問題は，長い歴史を持っています．それを説明するには，対数関数を定義する必要があります．

前に指数関数について述べました．$y = a$ がそれです．$a < 1$ として，この逆関数を

$$x = \log y$$

により表します．ただし，$y > 0$ とします．そして，これを（a を底とする）**対数関数**というのです．このグラフは次のようになりますね．



指数法則から，対数関数についての性質が導かれます．

$$\log_a(xy) = \log_a x + \log_a y, \quad x \log_a y = \log_a y^x$$

対数関数は，元々計算のために導入されたものです．すなわち，対数関数の表を用いて，積の演算を和の演算に直して計算しようというのが，元来の目的でした．その場合には，底 a としては，日常の計算では 10 を用います（常用対数）．

しかし，数学はもっと都合の良い底を取ります．それは自然対数の底と呼ばれるもので，次のように定義される数です．

$$\begin{aligned} e &= \lim_{n\to\infty}(1+\frac{1}{n})^n \\ &= 2.718281828459\cdots \end{aligned}$$

何故，このような底が数学で便利かというと，もし皆さんが関数の微分についてご存じなら，次のように説明できます．

関数 $y = e^x$ の導関数は，再び e^x となるのです．一般の指数関数 $y = a^x$ の導関数は

$$(\log_e a)a^x$$

となって，あまりきれいな式ではありませんね．e^x の導関数が e^x であることから，

$$e^x = 1 + x + \frac{1}{2\cdot 1}x^2 + \frac{1}{3\cdot 2\cdot 1}x^3 + \frac{1}{4\cdot 3\cdot 2\cdot 1}x^4 + \cdots$$

というように，美しい級数で表されることも分かります．普通は，$\log_e x$ の代わりに，e を省略して $\log x$ と書くことになっています．

さて，ルジャンドル (1803) は，次のような関数を考えました．

$$f(n) = \frac{n}{\log n - 1.08366\cdots}$$

そして

$$\#\mathrm{P}_n \sim f(n)$$

となることを予想したのです．$1.08366\cdots$ が現れるのはちょっと妙な気もします．

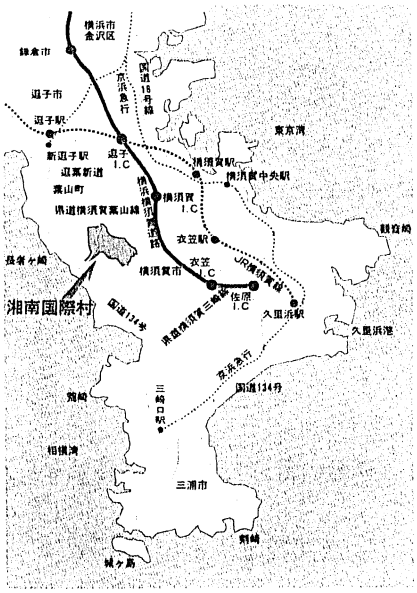
一方，前にも述べたガウスは 17 歳のとき (1792)，$f(n)$ として

$$f(n) = \frac{n}{\log n}$$

を考えればよいことを予想しました．どちらが正しかったのでしょうか．それはガウスです．実際，丁度 100 年前の 1896 年にプーサンとアダマールという数学者が同時にガウスの予想が正しいことを証明したのです．その証明には，前に定義したリーマンのゼータ関数の性質が用いられました．

素数とゼータ関数については，まだまだ述べたいことが沢山ありますが，ここで黒川先生にバトンタッチしましょう．

（すなだ　としかず，東北大学大学院理学研究科）



湘南国際村の位置