平方数和となる素数の正体

小山信也

1　証明したいこと

平方数の和となる素数について、私が初めて耳にしたのは、大学で整数論を専攻し始めて間もない頃であった。私の尊敬する指導教官の先生が、学生時代に彼女にふられた話をしてくださったときのことである。先生はその女性をめぐって歴史学科の友人とライバル関係にあったという。友人が専門の歴史の話題で彼女とのデートを盛り上げたのに対し、先生は数学の話題を切り出してみたものの受けるにはほど遠く、苦渋の青春時代を過ごされたとのことであった。

ふられはしたものの、そのとき先生が数ある数学の話題の中から彼女のために選んだとっておきのテーマが「平方数の和となる素数について」であった。さすがに選りすぐったテーマだけあって、この話題は整数論（類体論）における素イデアル分解法則の美しい一例であり、またゼータ関数の分解定理の実例にもなっている。類体論やゼータ関数論は現代の数学、整数論の結晶であり、高校数学の範囲で説明可能な題材により奥深い世界の入り口を垣間見られるのは、素晴らしいことだと思う。

「素数を二つの平方数の和に分けてみよう」と切り出した瞬間、彼女は「そんなことをして何になるの？」との疑問を抱いたそうである。そのような反応は人としてむしろ当然であり、今この瞬間にも多くの読者の皆さんがそのように感じているかも知れない。数学科の学生であった私ですら、先生がこの話を始められたとき「そんなことに何か意味があるのか?」との疑問を抱いたほどである。ところが、いくつかの素数について実例を知った途端、私の興味は掻き立てられた。

$$
\begin{aligned}
2 &= 1^2+1^2\\
3 &=\\
5 &= 1^2+2^2\\
7 &=\\
11 &=\\
13 &= 2^2+3^2\\
17 &= 1^2+4^2\\
19 &=\\
23 &=\\
29 &= 2^2+5^2\\
31 &=\\
37 &= 1^2+6^2\\
41 &= 4^2+5^2\\
43 &=\\
&\vdots
\end{aligned}
$$

左辺は上から素数を小さい順に並べている。右辺はその素数を二つの平方数の和として表したものである。ただし、そのように表せない場合は右辺を空欄とした。すると、右辺が空欄になっている素数には一つの共通点があることに気づく。それは、

右辺が空欄の素数はどれも、4 で割った余りが 3

ということである。逆に 4 で割った余りが 1 か 2（といっても余りが 2 となるのは最初の素数 2 のみであるが）であるような素数は、平方数の和として表されるようである。そしてこの法則は、素数をいくら大きくしても例外なく成り立つのだ。

ここまで聞いて、私は「これはただ事ではない」と思った。素数を 4 で割った余りと、素数が平方数の和で表せる可能性とは、元来はまったく関係ない事象である。この二つが結びついていることは不思議であり、何らかの理由があるに違いない。それまで抱いていた「何か意味があるのか」との疑問は「何らかの意味があるに違いない」との確信に変わり、ぜひともその意味を知りたいと思うに至った。

数学的にきちんと書くと次のようになる。

証明したいこと

p を 3 以上の素数とする。$p = x^2 + y^2$ を満たす整数 x, y が存在するための必要十分条件は、p を 4 で割った余りが 1 となることである。

必要十分条件を証明したいとき、必要条件と十分条件に分けて考えることは有効である。いずれか一方については簡単にわかってしまう場合も多い。必要と十分を分けて考えることで問題の本質が絞られる。今の場合、必要性、すなわち

$$p = x^2 + y^2 \text{ を満たす整数 } x, y \text{ が存在すれば、}$$
$$p \text{ を } 4 \text{ で割った余りが } 1$$

は、以下のように容易に証明できる。

必要性の証明：一般に偶数の 2 乗は $(2k)^2 = 4k^2$ より 4 の倍数であり、奇数の 2 乗は $(2k-1)^2 = 4(k^2-k)+1$ より 4 で割って 1 余る。したがって、$p = x^2 + y^2$ を 4 で割った余りは、x, y が共に偶数なら 0、一方が偶数で一方が奇数なら 1、共に奇数なら 2 となる。p は 3 以上の素数であるから奇数であり、したがって 4 で割った余りは 1 となる。（証明終）

今証明したことは、p を 4 で割った余りが 3 であるならば、$p = x^2 + y^2$ となるような x, y は存在しないということである。これで残るは十分性の証明のみとなった。すなわち、証明すべきことは次のことに絞られた。

証明したいこと（∗）

p を 3 以上の素数とする。p を 4 で割った余りが 1 であるならば、$p = x^2 + y^2$ を満たす整数 x, y が存在する。

2　存在証明の例：有限体の逆元

（∗）の証明が難しい一つの理由は、解 x, y の存在を証明しなければならない点であろう。現在、日本の高校などで習う数学では、解を求める場面は多いけれど解の存在を証明する場面は少ない。高校数学で見られる存在定理は「平均値の定理」（関数の平均変化率と微分係数の関係に関するもの）くらいだと思われるが、やはり難しいと感じている高校生が多いようである。

しかし、整数問題における存在定理は意外とやさしい。それは、整数は範囲を限れば有限個しかないことによる。有限個のものを扱うときは「部屋割り論法」という原理が使える。これは、存在を証明するために有用な論法である。空室 5 部屋のホテルに 6 人の客が来た場合、相部屋になる客が少なくとも 1 組**存在**する。あるいは、空室 5 部屋のホテルに 5 人の客が来てどの客も相部屋を拒んだ場合、どの部屋にも必ず客が**存在**する、というように用いる。

整数論では、たとえば次の命題の証明に用いられる。

有限体の逆元存在定理

素数 p の倍数ではない整数 a に対し、na を p で割った余りが 1 となるような整数 n が $1, 2, 3, ..., (p-1)$ の中に存在する。

証明：背理法で証明する。$(p-1)$ 個の整数 a, $2a$, $3a$,...,$(p-1)a$ の中に p で割った余りが等しいものがあると仮定する。それを ka と ma $(k \neq m)$ とおくと、$ka - ma = (k-m)a$ は p の倍数である。仮定より a は p の倍数でないから $k-m$ が p の倍数である。ところが k, m は $1, ..., (p-1)$ の中から選んでいるので、$k-m$ が p の倍数になることは

ありえない。よって背理法により、$(p-1)$ 個の整数 a, $2a$, $3a$,...,$(p-1)a$ は、p で割った余りがすべて異なる。すなわち、これらを p で割った余りの集合は $\{1, 2, 3, ..., (p-1)\}$ の全体と一致する。したがって部屋割り論法により、余りが 1 となるものが存在する。（証明終）

この証明は「p で割った余り」を部屋にたとえ、1 番から $(p-1)$ 番までの部屋に $(p-1)$ 個の数 na $(n = 1, 2, 3, ..., (p-1))$ を割り振ると考えている。証明の前半で、相部屋はありえないことを（背理法により）示し、したがってどれかの数が 1 番の部屋に入らなければならないと結論づけている。

これが逆元存在定理と呼ばれるのは、以下の理由による。整数を p で割った余りの集合 $\{0, 1, 2, ..., (p-1)\}$ に和、差、積の演算を、p で割る前の整数同士の演算により定義する。たとえば、$p = 5$ のとき、すべての整数を集合 $\{0, 1, 2, 3, 4\}$ の元に、5 で割った余りとして対応させた上で

$$3 + 4 = 7 = 2,$$
$$1 - 3 = -2 = 3,$$
$$3 \times 4 = 12 = 2,$$

などとするのである。このように等号の意味を拡張しておくと、上の逆元存在定理は、任意の a について

$$na = 1$$

なる元 n が存在することであり、これはすなわち乗法に関する a の逆元 a^{-1} の存在に他ならない。逆元をかけることを割り算とみなせば、この定理によって集合 $\{0, 1, 2, ..., (p-1)\}$ に四則演算が導入できたことになる。四則演算ができる集合を体と呼ぶ。有理数や実数、複素数の集合は体であるが、集合 $\{0, 1, 2, ..., (p-1)\}$ も体であり、これを有限体、または p 元体と呼ぶ。

さて、上の証明からすぐにわかることは、1 番の部屋に限らず、1 番から $(p-1)$ 番までのどの部屋にもどれかの数が必ず入っているということである。したがって、逆元存在定理は以下のような改良版も成立する。

有限体の逆元存在定理（改良版）

$1, 2, 3, ..., (p-1)$ の中の任意の整数 k と、素数 p の倍数ではない任意の整数 a に対し、na を p で割った余りが k （すなわち p 元体の中で $na = k$）となるような整数 n が $1, 2, 3, ..., (p-1)$ の中に存在する。

3　平方数和の正体

さて、ここで本来の目標**（∗）**に戻り、平方数和を改めて考えてみよう。平方数和とはいったい何なのか？ 高校までに習った数学を思い起こしながら、あり得る解法を並べ尽くしてみるうち、複素数に範囲を広げると

$$x^2 + y^2 = (x + iy)(x - iy)$$

と因数分解できることに気づく。こう書き換えたからといって直ちに問題が解けるわけではないが、p が素数であることと見比べると、この因数分解は特徴的であると感じられる。なぜなら、素数というのは、元来「それ以上分解できない整数」であったはずである。それなのにこの因数分解は、素数が複素数の範囲で

$$5 = (1 + 2i)(1 - 2i)$$

のように分解できてしまう（もはや素数ではない）ことを意味している。

素数が平方数の和に表されるとは、複素数の中ではもはや素数でないという意味であり、逆に平方数の和で表されないとは、複素数まで広げて考えてもなお素数であることを意味する。

すなわち、整数の範囲を複素数に広げたとき、4 で割って 3 余るような素数は素数であり続けるのに対し、4 で割って 1 余るような素数は素数でなくなってしまうということである。

4　虚数をもつ有限体

「素数がさらに分解される」という現象は、素数の本質をくつがえす衝撃的な事項であるともいえる。そこでこの現象について、少し詳しく考察してみたい。

複素数 i（虚数単位）を有限体で考えたらどうなるのだろうか。2 節で導入した演算を使って計算してみよう。i とは $x^2=-1$ の解であるが、$p=5$ のとき、有限体 $\{0,1,2,3,4\}$ の元の 2 乗を調べてみると

$$\begin{aligned}0^2&=0,\\1^2&=1,\\2^2&=4=-1,\\3^2&=9=-1,\\4^2&=16=1,\end{aligned}$$

となっている。これより、$x=2,3$ の二元が $x^2=-1$ の解であり、i と同様の性質をもつことがわかる。$x=2,3$ の一方を i と定めれば、他方はちょうど（5 元体の中で）$-i$ になっていることもわかる。実数から複素数を構成した際には新しい元 i を必要としたが、5 元体の場合はもともと i が存在しているのである。

そこで前節で得た素数の分解

$$p=x^2+y^2=(x+iy)(x-iy)$$

を $p=5$ の場合に $i=2$ とおいて書き直してみると、5 元体において成り立つ等式

$$5=(x+2y)(x-2y)$$

を得る。普通の整数の等式としてみると、両辺を 5 で割った余りが等しいという意味である。今、左辺が 5 であるから、この等式は右辺が 5 で割り切れることを意味している。実際、$(x,y)=(1,2)$ は $x+2y=5$ を満たす。

一般に方程式の整数解を求めるとき、まず両辺をある数で割った余りが等しいことを利用し、必要条件から解を絞っていく方法がある。方程式

$$p=x^2+y^2$$

を解く場合も、両辺を p で割った余りを考え、$x+iy$ が p の倍数になるような整数の組 (x,y) を探し、解の候補とするのが有効であろう。ただし、ここで i と書いたのは p 元体における $x^2=-1$ の解のことであり、$p=5$ ならば $i=2$ または $i=3$ である。

$x+iy$ が p の倍数になるような組 (x,y) を探すには、x,y について p で割った余りのみに注目すればよい。すなわち、組 (x,y) は p 元体の中で探せば十分であり、有限の範囲に限られた解を見つける方法として、2 節で述べた部屋割り論法が威力を発揮する。たとえば、p 元体の中で $x+iy$ の値が異なるような (x,y) が p 組以上になれば、$x+iy$ が p の倍数になるような解が存在する。

このアイディアを完成したものが以下の定理である。

有限体が虚数単位を含む場合の定理

p 元体が、$x^2=-1$ なる元 i を含んでいるとする。このとき、$x+iy$ が p の倍数であるような元 x,y が存在する。

証明：x,y を $0\le x<\sqrt{p},\ 0\le y<\sqrt{p}$ の範囲で渡らせると、(x,y) の組合わせの総数は $([\sqrt{p}]+1)^2$ であるから p 個以上となる。よって部屋割り論法により $x+iy$ を p で割った余りが等しくなるような (x,y) の組がある。これを $(x_1,y_1),(x_2,y_2)$ とおく。すなわち p 元体において

$$x_1+iy_1=x_2+iy_2$$

であり、変形して

$$(x_1-x_2)+(y_1-y_2)i=0$$

が成立する。普通の整数に戻して考えれば、$x=x_1-x_2,\ y=y_1-y_2$ に対して $x+iy$ が p の倍数であることを意味する。（証明終）

この定理によって方程式 $p=x^2+y^2$ の整数解 (x,y) の候補が見つけられたことになる。先の因数分解 $x^2+y^2=(x+iy)(x-iy)$ により、この候補は

$$x^2+y^2\text{ が }p\text{ の倍数}$$

という性質を満たす。一方、この定理の証明中で x, y を共に $\sqrt{p}$ 未満としていた。したがって、この (x, y) は実際には

$$x^2 + y^2 < 2(\sqrt{p})^2 = 2p$$

を満たしている。p の倍数でありかつ $2p$ より小さなものは p しかないので、$p = x^2 + y^2$ が成立する。これより以下の結論を得た。

有限体が虚数単位をもつ場合の結論

p 元体が、$x^2 = -1$ なる元 i をもつとする。このとき、

$$p = x^2 + y^2$$

の整数解 (x, y) が存在する。

5　4で割って1余る素数

これで、最終目標（∗）には、次を示せば到達することがわかった。

有限体が虚数単位をもつ条件

p を 3 以上の素数とする。p を 4 で割った余りが 1 であるならば、p 元体は、$x^2 = -1$ なる元 x をもつ。

これも有限の世界での話であるから、部屋割り論法により証明できる。ここでは 2 節で登場した定理を利用すると話が早い。

証明：2 節の「有限体の逆元存在定理」によると、1 以上 $p-1$ 以下の任意の整数 a に対し、1 以上 $p-1$ 以下の整数 n が存在して na を p で割った余りが 1 となる。この a と n を有限体の中でペアとみなす。$a = 1$ と $a = p - 1 = -1$ の二元だけは自分自身を逆数にもつためペアの相手がいないが、他のすべての元はペアの相手をもつ。したがって、$a = 1$ と $a = p-1$ の二元を除いた 2 から $p-2$ までをすべて掛け合わせた積 $(p-2)!$ を p で割った余りは、（先に各ペアで積を取ることにより）1 であるとわかる。よって、1 から $p-1$ までをすべて掛け合わせた積 $(p-1)!$ を p で割った余りは $p-1$ となる（この事実はウィルソンの定理として知られている）。

次に、2 節の末尾にある「有限体の逆元存在定理（改良版）」を、$k = -1$ として適用すると、1 以上 $p-1$ 以下の任意の整数 a に対し、1 以上 $p-1$ 以下の整数 n が存在して na を p で割った余りが -1 となる。今度はこの a と n をペアとみなす。証明すべきは、自分自身とペアになるような元 x の存在である。背理法で証明しよう。仮にこのような元が存在しないとすると、1 から $p-1$ までの整数たちは $\frac{p-1}{2}$ 組のペアからなっており、どの元もいずれかの組に属している。よって、1 から $p-1$ までをすべて掛け合わせた積 $(p-1)!$ を p で割った余りは（再び各ペアで先に積を取ることにより）$(-1)^{\frac{p-1}{2}}$ である。p を 4 で割った余りが 1 であることから $\frac{p-1}{2}$ は偶数となり、この余りの値は $(-1)^{\frac{p-1}{2}} = 1$ となる。一方、上記のウィルソンの定理によれば余りは $p-1$ のはずであったから、これは矛盾である。よって背理法により、自分自身とペアになるような元、すなわち $x^2 = -1$ なる元 x が存在する。（証明終）

6　ゼータの分解

前節までで最初の目標（∗）は完全に証明された。ところで、素数を知り尽くしているといわれているゼータ関数からは、この現象がどのようにみえるのだろうか。

ゼータ関数は素数全体にわたる積、または正の整数全体にわたる和により

$$\zeta(s) = \prod_{p:\text{素数}} (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (1)$$

と定義される。先の証明中で整数を複素数に拡張したので、この拡張した整数に対してもやはりゼータ関数を定義したい。複素数に拡張した整数（$x+iy$ で x, y が通常の整数であるもの）を「ガウス整数」と呼び、ガウス整数の全体の集合を $\mathbf{Z}[i]$ と書く。ゼータにこの記号をつけて表すことにすると、新しいゼータ関数 $\zeta_{\mathbf{Z}[i]}(s)$ を定義することが当面の目標である。

その際、最初に問題となるのが(1) の右辺の「正の整数」という概念である。複素数にはもともと正負がない。そこで右辺が整数全体の中から正の整数のみを取り出しているからくりをみてみると、これは整数全体の中で絶対値 1 の整数（すなわち ± 1）をかけたもの同士（たとえば 3 と -3）を一組とみなし、各組から代表として正のもの（すなわち 3）を取ったものと思える。そこでガウス整数に対しても、絶対値 1 のガウス整数 $\pm 1, \pm i$ をかけたもの同士（たとえば $\pm(1+2i)$ と $\pm(-2+i)$ の四元）を一組とみなし、各組から一つずつ代表が出せるような集合を求めればよい。これは、複素平面上で 90 度回転したものを同一視していることになるので、実軸の正の部分を 90 度回転したときに通る領域、すなわち $n+mi$ $(n=1,2,3,...,\ m=0,1,2,...)$ からなる集合が「正の整数」に相当すると考えればよいことがわかる。

次に、ゼータの拡張に必要な「ノルム」について説明する。前段落でみたように、正の整数とはあくまでも組の代表としての仮の姿であり、たとえば -3 という整数は無視されているわけではなく 3 に代表されているとみなされる。こうした事情を考慮すると、式(1) で n が複素数 $n+mi$ になった場合、そのまま複素数を用いてゼータを定義するのではなく、$n+mi$ の代表する四元からなる組の性質を反映した数 $N(n+mi)$（ノルムと呼ぶ）を定義して用いるべきであることがわかる。式(1) では 3 と -3 の組に対して正の数 3 をノルムとして採用していたことになる。これは、3 で割った余りの取り得る場合の数（-3 で割った余りでも同じ）である。すなわち、数直線上で 3 の倍数のすべてに印をつけたとき、隣り合う印を結んだ線分の内部および片端に存在する整数の個数であり、それは線分の長さに他ならない。そこで、$n+mi$ に対しても、ガウス整数を $n+mi$ で割った余りが取り得る場合の数を $N(n+mi)$ と定義する。この値を求めるには、数直線の場合にならって複素平面上で $n+mi$ の倍数に印をつけてみればよい。隣接する印のなす正方形、たとえば四元 $0,\ n+mi,\ i(n+mi),\ (1+i)(n+mi)$ を頂点とする正方形の内部およびいずれか一辺（端点は片側を含む）の上にあるガウス整数の個数がノルムであり、それはこの正方形の面積に他ならない。よって

$$N(n+mi) = \left(\sqrt{n^2+m^2}\right)^2 = n^2+m^2$$

であることがわかる。これを用いて、ゼータ(1) のガウス整数への拡張を

$$\zeta_{\mathbf{Z}[i]}(s) = \prod_{P:\text{ガウス整数の素数}} (1-N(P)^{-s})^{-1} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} \frac{1}{N(n+mi)^s} \tag{2}$$

と得る。2 つのゼータ (1)(2) を見比べてその関係を求めてみよう。

まず素数 p が 4 で割って 1 余る場合、3 節でみたように p はガウス整数としては素数ではなく、2 つのガウス整数の素数の積に $p=(x+iy)(x-iy)$ と分解される。この場合、(1) の p の因子に対応して (2) に $P=x+iy$ と $\bar{P}=x-iy$ の因子があることになる。$N(P)=N(\bar{P})=x^2+y^2=p$ であるから、(2) の $P, \bar{P}$ の因子は同じになり、その積は平方

$$(1-N(P)^{-s})^{-1}(1-N(\bar{P})^{-s})^{-1} = (1-p^{-s})^{-2} \tag{3}$$

により表される。すなわち (1) の p 因子に対応する部分として、(2) では同じ因子が 2 つあることになる。

次に素数 p が 4 で割って 3 余る場合、3 節でみたように p はガウス整数としても素数である。よって、(1) の p 因子に対応して (2) にも $P=p$ の因子がある。$N(p)=p^2$ であるから、(2) の P 因子は

$$(1-N(P)^{-s})^{-1} = (1-p^{-2s})^{-1} = (1-p^{-s})^{-1}(1+p^{-s})^{-1} \tag{4}$$

と因数分解され、これは (1) の p の因子に符号を一箇所変えた新しい因子 $(1+p^{-s})^{-1}$ をかけたものになっている。

残る $p=2$ の場合は例外的であり、これだけ別に計算する。ガウス整数としての素因数分解は $2=-i(1+i)^2$ となることが知られている。$p=2$ に対

応する因子は $P=1+i$ となり、$N(1+i)=2$ となるから (1)(2) のゼータの因子は同一で共に

$$(1-2^{-s})^{-1} \tag{5}$$

であることがわかる。

ガウス整数のゼータ (2) は、(3)(4)(5) の各型の因子の積であるから、

$$\zeta_{\mathbf{Z}[i]}(s)=\zeta(s)L(s,\chi) \tag{6}$$

のように分解されることがわかる。ここで

$$L(s,\chi)=\prod_{p:\text{素数}}(1-\chi(p)p^{-s})^{-1}$$

であり、これはゼータ (1) の各 p 因子の式中の符号を

$$\chi(p)=\begin{cases}1 & (4\text{で割って}1\text{余る}p\text{のとき})\\ -1 & (4\text{で割って}3\text{余る}p\text{のとき})\\ 0 & (p=2\text{のとき})\end{cases}$$

を用いて修正したものである。χ はクロネッカー記号、ルジャンドル記号などと呼ばれるものであり、ディリクレ指標の一例である。$L(s,\chi)$ は指標 χ に関するディリクレ L-関数と呼ばれ、ゼータの一種である。

7 発展

ここまで扱ってきた話題は、いろいろな方向に発展させることができる。美しい真理を初めて見出すことが数学の醍醐味であるのはいうまでもないが、その後にそこから様々な類似や一般化を得るのもまた数学の喜びであろう。

もっとも素朴な発展は「p が素数」という条件を外し、一般の整数 n に対して平方数和の式 $n=x^2+y^2$ の整数解を考えることであろう。この整数解の個数は n の素因数分解において、4 で割って 1 余る素因数と 3 余る素因数の登場の仕方によって書き表すことができる（ルジャンドルの 2 平方和定理、文献 [4], p.245）。

さらに、$p=x^2+y^2$ を $p=x^2+2y^2$、$p=x^2-3y^2$ などに形を変えてみると、いろいろな事実がわかる。たとえば前者の場合、整数解は p を 8 で割った余りが 1 または 3 のときは存在するが、5 または 7 のときは存在しない。そしてこれを踏まえた上で再び p が素数であるという条件を外し、ルジャンドルの 2 平方和定理の一般化を得ることもできる (文献 [2])。このあたりの話題は初等整数論だけを用いながら類似・一般化という数学研究の経験が実感できる絶好の題材である。文献 [2] が当時大学 1 年の著者によって 1 学期に書かれたものであるという事実は、多くの高校生や数学研究を趣味とされる方々の励みになることであろう。

以上はいわば初等整数論の範囲内での発展であったが、さらに高度な整数論の立場からは、本稿のテーマは「代数体の拡大における整数環の素イデアルの分解定理」と位置付けられる。代数体として特に $\mathbf{Q}(i)$ をとれば $p=x^2+y^2$ が解け、$\mathbf{Q}(\sqrt{-2})$ をとれば $p=x^2+2y^2$ が解ける。これらはいずれも 2 次体という、拡大体の中でもっとも簡単なものである。一般の拡大体に関する理論は類体論と呼ばれており、特にアーベル拡大に関する理論は現代数学でもっとも美しい成果の一つとされている (文献 [1])。

さらに、ガウス整数環のゼータ関数 (2) も一般の代数体に定義を拡張でき、デデキント・ゼータと呼ばれている（それに対して元来の (1) をリーマン・ゼータと呼ぶ)。分解定理 (6) も一般化され、アーベル n 次拡大のデデキント・ゼータは n 個の $L(s,\chi)$ や $\zeta(s)$ の積にきれいに分解される。非アーベル拡大に対してはアルティンの L-関数、ヘッケの L-関数、さらに保型形式の L-関数など、より多彩なゼータたちが関係してくる。そしてそれらのゼータたちは数多くの未解決問題 (文献 [3]) を携え、人々の来訪を待っているのである。

参考文献

[1] 加藤和也・黒川信重・斎藤毅：「数論 1」（岩波書店）

[2] 加藤祐子:「自然数を $N = A^2+2B^2$ と表す方法の総数」（数学研究法セミナー報告集、ゼータ研究所）http://www1.tmtv.ne.jp/~koyama/

[3] 小山信也:「リーマン予想」数学セミナー 2000 年 11 月号（日本評論社）

[4] ジョセフ・H・シルバーマン：「はじめての数論」（ピアソン・エデュケーション）