数論における3大予想について

吉　本　明　宣

1．はじめに

学問の中でも最も長い伝統をもつもののひとつである数学の歴史は、ギリシャ文明の時代にすでにユークリッドの「幾何学原論」という形で花開いていた。そこでは初等幾何学と初等数論が展開された。この「幾何学原論」はその後数学を含むいろいろな学問の基本となった。ニュートンの「プリンキピア」もこの本の影響のもとに書かれている。こうして数学は、哲学に近い形で誕生し、自然科学の基礎としての役割りを果たしてきただけでなく、実用的にも測量術からコンピューターまでさまざまなものを作りだしてきた。

高度に進化した現代の純粋数学は実生活とはあまり密着していない。しかし数学は自然、社会、人文科学におけるいろいろな現象を説明する言葉として不可欠なものになっている。純粋数学が扱う数学的自然の対象は、大きく分けて3つに分類される。大きさ（解析）、形（幾何）、数（数論）がそれである。本稿においては話を数論にしぼり、過去・現在・未来において最も重要だと思われる3大予想について、その歴史と今後の解決の可能性について論じてみたい。

2．リーマン予想

2．1　リーマンのゼータ関数

s を複素数とし、$Re(s)>1$ のとき絶対収束するディリクレ級数

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

で表わされる関数をリーマンのゼータ関数という。$\zeta(s)$ は容易にわかる様に次のオイラー積をもつ。

$$\zeta(s)=\prod_{p}(1-p^{-s})^{-1}\qquad(p\text{ は素数全体を動く})\tag{2.1}$$

$\zeta(s)$ は $Re(s)>1$ で絶対かつ広義一様収束するので、この範囲で s に関する正則関数になっているが、定義域を拡張することを考える。そこでガンマー関数

$$\Gamma(s)=\int_0^{\infty}e^{-t}t^{s-1}\,dt$$

を使ってこれを行う。a を正の数とし、この式で $t\to at$ なる変換をすると、

$$\Gamma(s)=a^s\int_0^{\infty}e^{-at}t^{s-1}\,dt\tag{2.2}$$

となる。よって

$$\frac{1}{a^s}=\frac{1}{\Gamma(s)}\int_0^{\infty}e^{-at}t^{s-1}\,dt\tag{2.3}$$

を得る。(2. 3) を使うと、$Re(s) = \sigma > 2$ のとき

$$\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \Gamma\left(\frac{s}{2}\right)\sum_{n=1}^{\infty}\frac{1}{(\pi n^2)^{s/2}}$$

$$= \lim_{N\to\infty}\int_0^{\infty}\left(\sum_{n=1}^{N} e^{-\pi n^2 t}\right) t^{\frac{s}{2}-1}\,dt$$

となる。ところが、$Re(s) = \sigma > 2$ であるから、

$$\int_0^{\infty}\left|\left(\sum_{n=N+1}^{\infty} e^{-\pi n^2 t}\right) t^{\frac{s}{2}-1}\right| dt$$

$$\leqq \int_0^{\infty}\sum_{n=1}^{\infty} e^{-\pi(N+1)nt}\, t^{\frac{\sigma}{2}-1}\,dt$$

$$= \int_0^{\infty} e^{-(N+1)^2\pi t}\{1 - e^{-(N+1)\pi t}\}^{-1} t^{\frac{\sigma}{2}-1}\,dt$$

$$\leqq \{(N+1)\pi\}^{-1}\int_0^{\infty} e^{-(N+1)^2\pi t}\, t^{\frac{\sigma}{2}-2}\,dt$$

$$= \{(N+1)\pi\}^{-1}\{(N+1)^2\pi\}^{1-\frac{\sigma}{2}}\,\Gamma\left(\frac{\sigma}{2}-1\right)$$

$$\to 0 \quad (N\to\infty)$$

となる。よって積分の中と外の $\sum$ の交換ができ、

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^{\infty}\left(\sum_{n=1}^{\infty} e^{-\pi n^2 t}\right) t^{\frac{s}{2}-1}\,dt \qquad (2.\ 4)$$

を得る。ここで積分の中にでてくる

$$\theta(t) = \sum_{n=1}^{\infty} e^{-\pi n^2 t} \quad (t > 0)$$

はテータ関数とよばれ、数論では最も基本的でかつ重要な関数である。このテータ関数は次の変換公式を満たす。

$$1 + 2\theta(t) = t^{-\frac{1}{2}}\left\{1 + 2\theta\left(\frac{1}{t}\right)\right\} \qquad (2.\ 5)$$

そこで次の 2. 2 の中でこの変換公式を証明し、$\zeta(s)$ の定義域の拡張の残りの部分を解説したい。

2．2　関数等式とテータ関数

リーマンのゼータ関数は関数等式

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \qquad (2.\ 6)$$

を満たすが、これを証明するために (2. 5) の変換公式を証明し、$\zeta(s)$ の解析接続を与えなければならない。まず (2. 5) の等式を証明する。x を実数とし、$\Phi(x)$ を実数上の急減少関数とする。すなわち $\Phi(x)$ は無限回微分可能で、任意の自然数 m、n に対して、

$$|\Phi^{(m)}(x)| \leqq \frac{1}{|x|^n} \quad (|x| \text{が十分大きいとき})$$

とする。そのとき $\Phi(x)$ は次のポアッソンの和公式

$$\sum_{n=-\infty}^{\infty}\Phi^*(n) = \sum_{n=-\infty}^{\infty}\Phi(n) \qquad (2.\ 7)$$

を満たす。ここで $\Phi^*(y)$ (y は実数) は y のフーリエ変換

$$\Phi^*(y) = \int_{-\infty}^{\infty} \Phi(x)\, e^{2\pi i x y} dx$$

である。この和公式は解析の非常に基本的な式であり、証明は難しくないが省略する。よく知られている性質

$$e^{-\pi y^2} = \int_{-\infty}^{\infty} e^{-\pi x^2} e^{2\pi i x y} dx \tag{2.8}$$

により

$$e^{-\pi \frac{y^2}{t}} = t^{-\frac{1}{2}} \int_{-\infty}^{\infty} e^{-\pi x^2 t} e^{2\pi i x y} dx \tag{2.9}$$

が得られ、(2.7) の $\Phi(x)$ として $e^{-\pi x^2 t}$ を代入することにより (2.5) の変換公式が導き出される。

次に解析接続と関数等式について述べよう。(2.4) により

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_0^1 \theta(t)\, t^{\frac{s}{2}-1} dt + \int_1^{\infty} \theta(t)\, t^{\frac{s}{2}-1} dt$$

$$= \int_0^1 \left\{ -\frac{1}{2} + \frac{1}{2} t^{-\frac{1}{2}} + t^{-\frac{1}{2}} \theta\left(\frac{1}{t}\right) \right\} t^{\frac{s}{2}-1} dt + \int_1^{\infty} \theta(t)\, t^{\frac{s}{2}-1} dt$$

を得る。上の2つ目の等号で (2.5) を使った。さらに、第一の積分で $t \to 1/t$ とすると、

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \frac{1}{s(s-1)} + \int_1^{\infty} \left(t^{\frac{1-s}{2}} + t^{\frac{s}{2}}\right) t^{-1} \theta(t)\, dt \tag{2.10}$$

となる。上式の積分は、任意の複素数 s に対して収束し、s の正則関数となる。従って $\zeta(s)$ は全平面の有理型関数である。極の可能性は $s = 0, 1$ であるが、$s = 1$ では明らかに留数1の極となる。ところが、ガンマ関数の性質により $s = 0$ では正則となる。また (2.10) の表示は $s \to 1 - s$ なる変換で不変であるから、(2.6) の関数等式も得られた。

この節の最後にリーマンのゼータ関数の零点について述べてみたい。$\zeta(s)$ はオイラー積をもつことにより、$Re(s) > 1$ では零点を持たない。また関数等式 (2.6) により、$Re(s) < 0$ でも零点をもたない（自明な零点を除いて）ことがわかる。従って $\zeta(s)$ の零点は $0 \leqq Re(s) \leqq 1$ にあることになるが、$Re(s) = 1$ 上に零点がないことにより素数定理が導かれる。それ以外に本質的な事はほとんどわかっていない。にもかかわらず、リーマンは1859年にリーマン予想と呼ばれる予想を提出した。これは数学史上最大難問とも言われ、すでに予想提出から百余年の年月が経過しているが、現時点において解決に際して何の手がかりも得られておらず、もしリーマン予想が正しければ、素数の詳しい分布など多くの事実が得られることだけがわかっている。

3．アルティン予想

k を有限次代数体、K を k の有限次ガロア拡大で、$G = G(K/k)$ をそのガロア群とする。$\sigma \to A(\sigma)$ を G から $GL(n, C)$ への写像で、

$$A(\sigma\tau) = A(\sigma) A(\tau)$$

を満たすものとする。$\chi(\sigma) = trA(\sigma)$ とおく。

k の素イデアル $\mathfrak{p}$ と、$\mathfrak{p}$ の k へのある延長 $\mathfrak{P}$ に対し、$N\mathfrak{p}$ を $\mathfrak{p}$ のノルムとし、$F_{\mathfrak{P}}$ を

Gの元で、Kの任意の整数の$\alpha \in \mathfrak{O}_K$（$K$の整数環）に対し、

$$\alpha^{\sigma} \equiv \alpha^{N\mathfrak{P}} \pmod{\mathfrak{P}}$$

を満たすσの全体とする。そこで

$$A_{\mathfrak{P}} = \#(F_{\mathfrak{P}})^{-1} \sum_{\sigma \in F_{\mathfrak{P}}} A(\sigma) \in M_n(\boldsymbol{C})$$

$$L_{\mathfrak{P}}(s, \chi) = det(1 - A_{\mathfrak{P}} N(\mathfrak{P})^{-s})$$

とおく。$L_{\mathfrak{P}}(s, \chi)$は$\mathfrak{P}$にのみより、$\mathfrak{P}$の延長$\mathfrak{P}$のとり方によらず決まる。そこでさらにすべての$\mathfrak{P}$に関する積をとり、

$$L(s; \chi, K/k) = \Pi L_{\mathfrak{P}}(s, \chi)$$

とおき、これをガロア群$G(K/k)$の指標$\chi(\sigma)$に対するアルティンのL関数とよぶ。

$L(s; \chi, K/k)$は$Re(s) > 1$で定義された正則関数であり、オイラー積をもつ。とくに$G(K/k)$がアーベル群の場合には、類体論により、$L(s; \chi, K/k)$はkのあるヘッケの類指標χに対するヘッケのL関数$L(s; \chi)$に等しくなる。

一般に$G(K/k)$がアーベル群とは限らない場合には、ブラウアーの定理により、$K \supseteq k_i \supseteq k$なる体$k_i$ $(i = 1, \cdots, t)$と、k_iのヘッケのL関数$L(s; \chi_i)$があり、

$$L(s; \chi, K/k) = \prod_{i=1}^{t} L(s; \chi_i)^{e_i} \quad (e_i \in \boldsymbol{Z})$$

とかける。これにより$L(s; \chi, K/k)$が有理型関数に拡張され、関数等式をもつことがわかる。アルティン予想とは次のものである。

予想：$\sigma \to A(\sigma)$が既約で、かつ$A(\sigma) \neq 1$の場合には、$L(s; \chi, K/k)$は$\boldsymbol{C}$上で解析的（正則）である。

この予想は、類体論（アーベル拡大体に関するイデアルの分解法則を述べた理論）の非アーベル拡大体の場合に関する一般化を述べたものである。アルティンは、アルティンのL関数を研究する過程で、高木の類体論を使うことによりアルティンの相互律を発見した。さらに、アルティンの相互律を直接証明し、類体論の建設に大きく貢献した。それは1920年代の事であるが、その後類体論を中心に数論は展開され、アルティンのL関数は表理論やガロア群の研究に多大な影響を及ぼした。しかし、解決に到達するには本質的な飛躍が必要である。

4．フェルマー予想

4．1　フェルマー予想

フェルマーは1637年頃ディオファンタスの「数論」という本を読んで刺激を受け、不定方程式の研究を始めたと言われている。その書の中のピタゴラス数（$x^2 + y^2 = z^2$を満たす整数の組）を述べてあるページの欄外に、いわゆるフェルマーの大定理（フェルマー予想）が書き込まれていた。それは次のようなものであった。

フェルマー予想：nを2より大きな自然数とすると、方程式

$$x^n + y^n = z^2$$

は自明な解以外は整数解をもたない。

この予想がフェルマーの大定理といわれる理由は、フェルマーが、「私はこの欄外では狭すぎて書き切れないまことに驚嘆すべき証明を見つけた」と記したからである。しかし、この問題は現在でも未だ解決されていない大予想であり、数学の多くの分野がこの問題を契機に発展している。例えば代数的整数論におけるイデアル論などは、その典型である。$n=3$ の場合は代数的整数の知識を必要とするので、ここでは $n=2$ の場合と $n=4$ の場合について論じてみたい。無論それ以外の場合は非常に難しい。

まず $n=2$ の場合を考えてみよう。このときはフェルマー予想には含まれず、自明でない解が存在する。上で述べたようにそれはピタゴラス数とよばれている。$x^2+y^2=z^2$ の整数解を考えることは、$X^2+Y^2=1$ の有理数解を考えることと同じである。そこで $X^2+Y^2=1$ と $Y=tX-1$ の交点を求めてみると、

$$X=\frac{2t}{t^2+1},\quad Y=\frac{t^2-1}{t^2+1}$$

となる。ゆえに $t=b/a$ とすれば (a, b は整数、$a\neq 0$)

$$X=\frac{2ab}{a^2+b^2},\quad Y=\frac{a^2-b^2}{a^2+b^2}$$

となり、$x=2ab$、$y=a^2-b^2$、$z=a^2+b^2$ は $x^2+y^2=z^2$ の解となる。このことを使って $n=4$ の場合を証明してみよう。

証明　　$x^4+y^4=z^2,\ (x,y)=1$　　(4. 1)

に自然数解がないことをいえば十分である。(4. 1) に自然数解 (x, y, z) があったとすると、

$$(x^2)^2+(y^2)^2=z^2$$

となる。だから、(x^2, y^2, z) はピタゴラス数である。従って、

$$x^2=2ab,$$
$$y^2=a^2-b^2,$$
$$z=a^2+b^2$$

と表わせる。ここに $a>b>0$ かつ $(a, b)=1$ である。上の第2式より $b^2+y^2=a^2$ で、$(b, y)=1$ かつ (y が奇数だから) b は偶数であって、

$$b=2cd,$$
$$y=c^2-d^2,$$
$$a=c^2+d^2$$

$(c>d>0,\ (c, d)=1)$ なる c, d が存在する。ゆえに

$$x^2=2ab=4cd\,(c^2+d^2)$$

となる。c, d, c^2+d^2 は互いに素だから、上式は、c, d, c^2+d^2 がどれも平方数であることを意味する。ゆえに

$$c=e^2,$$
$$d=f^2,$$
$$c^2+d^2=g^2$$

となる e, f, g が存在する。従って

$$e^4 + f^4 = g^2, \ (e, f) = 1$$

を得る。つまり (e, f, g) は (4. 1) を満足する。

$$z = a^2 + b^2 > a^2 = (c^2 + d^2) = g^4 > g > 0$$

だから $z > g > 0$ である。z を (4. 1) を満たす x, y, z のうちで最小になるようにとっておけば、これは矛盾である。ゆえに (4. 1) には自然数解は存在しない。

以上が $n = 4$ の場合の証明であり、無論これ以外の証明はいくつもある。一般の場合の研究は、現在でも盛んに行われており、代数幾何学、超越数論などを使って現在の最先端の数学が展開されている。次の (4. 2) においてごく簡単にこの話題に触れてみることにする。

4．2　モーデル予想

$f(x, y)$ を 2 変数整係数多項式とする。$f(x, y)$ から定まる滑らかな閉曲面の穴の数 g を種数という。モーデルは、1922年の論文で $g = 1$ の場合の $f(x, y) = 0$ の有理数解の構造を決定した。その論文の最後に、彼は次のような予想を述べた。

モーデル予想：$f(x, y) = 0$ の定める閉曲面が $g > 1$ の射影曲線ならば、有理数解は有限個である。

この予想は1983年にファルティンクスによって解かれ、日本でも大変な騒ぎになった。前に述べたフェルマー予想の多項式の定める閉曲線は $g > 1$ なので、有理数解は有限個であることはこれでわかったわけであるが、自明な解以外は存在しないという部分に到達するにはまだ少しギャップがあるような気がする。最近、超越数論の人達がこの有限性を評価しようと試みており、ひょっとしたらうまくいくかもしれない。

5．クロネッカーの青春の夢

5．1　平方剰余の相互法則

p を奇素数とする。p と互いに素な整数 a に対して、合同式

$$X^2 \equiv a \ (\mathrm{mod} p)$$

が解をもつとき、a は法 p に関する平方剰余であるといい、

$$\left(\frac{a}{p}\right) = 1$$

とかく。また解をもたないときには、a は法 p に関する平方非剰余であるといい、

$$\left(\frac{a}{p}\right) = -1$$

とかく。この記号 $\left(\frac{a}{p}\right)$ を平方剰余記号またはルジャンドルの記号という。そのとき平方剰余の相互法則とは次の法則をいう。

平方剰余の相互法則：p, q を相異なる奇素数とするとき、

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

が成立する。

証明　　F_p を p 個の元から成る有限体とする。そこでガウス和

$$G=\sum_{a=1}^{q-1}\left(\frac{a}{q}\right)\eta^a=\sum_{a\in F_q^\times}\left(\frac{a}{q}\right)\eta^a$$

を考える。ここで η は 1 の原始 q 乗根の 1 つで、$F_q^\times=F_q-\{0\}$ である。

$$G^2=\left(\sum_{a\in F_q^\times}\left(\frac{a}{q}\right)\eta^a\right)\left(\sum_{b\in F_q^\times}\left(\frac{b}{q}\right)\eta^b\right)=\sum_{a,\,b\in F_q^\times}\left(\frac{ab}{q}\right)\eta^{a+b}$$

に対して、$a\neq 0$ より $b=ac$, $c\in F_q^\times$ とおくと、

$$G^2=\sum_{a,\,c\in F_q^\times}\left(\frac{a^2c}{q}\right)\eta^{a(1+c)}=\sum_{c\in F_q^\times}\left(\frac{ab}{q}\right)\eta^{a+b}$$

となる。ここで、$e\in F_q^\times$ に対して、

$$\sum_{a\in F_q^\times}\eta^{ae}=\begin{cases}q-1 & (e=0)\\ -1 & (e\neq 0)\end{cases}$$

に注意すると、

$$G^2=\left(\frac{-1}{q}\right)(q-1)-\sum_{c\neq 0,\,1}\left(\frac{c}{q}\right)=\left(\frac{-1}{q}\right)q$$

を得る。従って $q'=\left(\frac{-1}{q}\right)q$ とおくと、

$$G^p=(G^2)^{\frac{p-1}{2}}\cdot G=(q')^{\frac{p-1}{2}}\cdot G=\left(\frac{q'}{p}\right)\cdot G$$

となる。ここでオイラーの規準 $(q')^{\frac{p-1}{2}}=\left(\frac{q'}{p}\right)$ を使った。一方

$$\begin{aligned}G^p&=\left(\sum_{a\in F_q^\times}\left(\frac{a}{q}\right)\eta^a\right)^p\\&=\sum_{a\in F_q^\times}\left(\frac{a}{q}\right)^p\eta^{ap}\\&=\left(\frac{p}{q}\right)\sum_{a\in F_q^\times}\left(\frac{ap}{q}\right)\eta^{ap}\\&=\left(\frac{p}{q}\right)G\end{aligned}$$

となる。ゆえに

$$\left(\frac{q'}{p}\right)G=\left(\frac{p}{q}\right)G$$

が成り立つ。$G\neq 0$ より

$$\left(\frac{q'}{p}\right)=\left(\frac{p}{q}\right)$$

が得られる。従って、証明すべき

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

を得る。

上の証明はガウスによってなされたもので、ガウスはこの法則に 7 つの証明を与えている。それらは現在研究されている数論の基礎となるもので、現在の数論はすべてそれらの証明から発生しているといっても過言ではない。ガウスが執拗なまでにこの定理の証明に

こだわったのは、平方剰余に続く高巾剰余の相互法則の手がかりをつかむためであった。残念ながらガウスはそれを完全には得ることはできなかったが、19世紀の数論学者達はその遺産を受け継ぎ、ついに1920年代の高木およびアルティンの類体論の完成によって、完全な証明が与えられた。上に述べた平方剰余の相互法則は有理数体の場合におけるものである。次に任意の代数体において平方剰余の相互法則を考えたいと思う。そしてその法則に比較的見通しの良い証明を与えたい。

5．2　一般の有限次代数体における平方剰余の相互法則

Fを有限次代数体とし、a, bをFの代数的整数としたとき、$\left(\frac{b}{a}\right)$によってFの平方剰余記号を表わす。ただし、分母のaは2と互いに素なものだけを考える。ここで我々が証明しようとしている平方剰余の相互法則とは次のものを言う。

平方剰余の相互法則：α, β, β'はFの代数的整数であるとする。そのとき、$(\beta\beta', 2\alpha)=1, \beta \equiv \beta' \pmod{4\alpha}$ならば

$$\left(\frac{\alpha}{\beta}\right)=\left(\frac{\alpha}{\beta'}\right)$$

が成り立つ。

これを証明するにはいろいろな準備が必要である。多少複雑になるかもしれないが、ここで与える証明はわかりやすいと思う。

Fの次数をnとし、Fの実の共役の数をr_1、虚の共役の数をr_2とする。従って$n=r_1+2r_2$である。$\mathfrak{O}$をFの整数環とする。Fは共役によって$V=\boldsymbol{R}^{r_1}\times\boldsymbol{C}^{r_2}$にうめこめる。そのとき$F$の元$x$を$x=(x^{(1)}, \cdots, x^{(r_1)}, x^{(r_1+1)}, \cdots x^{(r_1+r_2)})$で表わすことができる。また$V/\mathfrak{O}$はコンパクトになる。そこで、

$$\Gamma(4)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\mathfrak{O}) \,\middle|\, \begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \pmod{4}\right\} \tag{5.1}$$

とおき、$\sigma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma(4)$に対して

$$x(\sigma)=\begin{cases}\left(\frac{2c}{a}\right) & (c\neq 0),\\ 1 & (c=0)\end{cases} \tag{5, 2}$$

と定義する。そのとき1)よりχが$\Gamma(4)$の指標になることと、平方剰余の相互法則は同値になる。この証明はそれほど難しくはないが、省略する。また

$$trx=\sum_{p=1}^{r_1+r_2} tr_R x^{(p)}, \quad e(x)=\exp(2\pi i trx)$$

とおく。$\Phi(x)$をVの関数で、$\boldsymbol{R}^n$の関数とみたときに急減少関数であるとする。$\Phi(x)$に対してフーリエ変換$\Phi^*(y)$ $(y\in V)$を次のように定義する。

$$\Phi^*(y)=\int_V \Phi(x)\, e(xy)\, dx,$$

ここで$dx=dx^{(1)}\cdots dx^{(r_1)}\,|\,dx^{(r_1+1)}\wedge d\overline{x^{(r_1+1)}}\,|\cdots|\,dx^{(r_1+r_2)}\wedge d\overline{x^{(r_1+r_2)}}\,|$である。$\vartheta$を$F$のdifferentとする。

$$F(x) = \sum_{m \in \mathfrak{G}} \Phi(x+m)$$

とおくと、任意の $c \in \mathfrak{G}$ に対して $F(x+c) = F(x)$ となる。フーリエの変換公式

$$\int_{(V/\mathfrak{G})^*} \int_{V/\mathfrak{G}} F(x)\, e(xy)\, dx\, e(-yz)\, d^*y = F(z) \tag{5.3}$$

を使う。ここで $(V/\mathfrak{G})^* = \{y \in V \mid$ 任意の $x \in V/\mathfrak{G}$ に対して $e(xy) = 1\}$, d^*y は $(V/\mathfrak{G})^*$ のハール測度である。$F(x) \equiv 1$ ($V/\mathfrak{G}$ の上で) とすると、$v(V/\mathfrak{G}) \cdot d^*y\{0\} = 1$ である。ここで $v(V/\mathfrak{G})$ は $V/\mathfrak{G}$ の体積である。従って

$$d^*y\{0\} = (|d|^{\frac{1}{2}})^{-1} \quad (d : F \text{の判別式})$$

となる。また $(V/\mathfrak{G})^* \cong \mathfrak{H}^{-1}$ だから

$$F(x) = |d|^{-\frac{1}{2}} \sum_{n \in \mathfrak{H}^{-1}} \left(\int_{V/\mathfrak{G}} F(x)\, e(xn)\, dx \right) e(-nz) \tag{5.4}$$

となる。ここで $F(z) = \sum_{m \in L} \Phi(z+m)$ とすると、

$$\begin{aligned} F(z) &= |d|^{-\frac{1}{2}} \sum_{n \in \mathfrak{H}^{-1}} \left(\int_{V/\mathfrak{G}} \sum_{m \in L} \Phi(x+m)\, e(xn)\, dx \right) e(-nz) \\ &= |d|^{-\frac{1}{2}} \sum_{n \in \mathfrak{H}^{-1}} \left(\int_{V} \Phi(x)\, e(xn)\, dx \right) e(-nz) \\ &= |d|^{-\frac{1}{2}} \sum_{n \in \mathfrak{H}^{-1}} \Phi^*(n)\, e(-nz) \end{aligned}$$

を得る。上式において $z = 0$ とすれば、

$$\sum_{m \in L} \Phi(m) = |d|^{-\frac{1}{2}} \sum_{n \in \mathfrak{H}^{-1}} \Phi^*(n) \tag{5.5}$$

が得られる。

ここで上半平面 $H = \{(u, v) \mid u \in \boldsymbol{R},\ v > 0\}$ を考えると、H の元 (u, v) は $\begin{pmatrix} u & -v \\ v & u \end{pmatrix}$ と同一視できるから、$SL(2, \boldsymbol{R})$ の H への作用を次のように定義する。

$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{R})$, $z = \begin{pmatrix} u & -v \\ v & u \end{pmatrix}$ に対して、

$$\sigma(z) = (\tilde{a}z + \tilde{b})(\tilde{c}z + \tilde{d})^{-1} \tag{5.6}$$

とする。ここで $\tilde{u} = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$ $(u \in \boldsymbol{R})$ である。

同様にして上半空間 $\hat{H} = \{(z, v) \mid z \in \boldsymbol{C},\ v > 0\}$ を考えると、$\hat{H}$ の元 $w = (z, v)$ は $\begin{pmatrix} z & -v \\ v & \bar{z} \end{pmatrix}$ と同一視できるから、$SL(2, \boldsymbol{C})$ の $\hat{H}$ への作用を次のように定義する。

$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{C})$, $w = \begin{pmatrix} z & -v \\ v & \bar{z} \end{pmatrix}$ に対して、

$$\sigma(w) = (\tilde{a}w + \tilde{b})(\tilde{c}w + \tilde{d})^{-1} \tag{5.7}$$

とする。ここで $\tilde{z} = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$ $(z \in \boldsymbol{C})$ である。

そこで、$F \subset V = \boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$ であるから、$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(4)$ に対してその共役を

$$\sigma_1 = \begin{pmatrix} a^{(1)} & b^{(1)} \\ c^{(1)} & d^{(1)} \end{pmatrix}, \quad \cdots, \quad \sigma_{r_1+r_2} = \begin{pmatrix} a^{(r_1+r_2)} & b^{(r_1+r_2)} \\ c^{(r_1+r_2)} & d^{(r_1+r_2)} \end{pmatrix}$$

とする。従って $\Gamma(4)$ の $H^{r_1} \times \widehat{H}^{r_2}$ への作用を、$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(4)$, $w = (w_1, \cdots, w_{r_1+r_2}) \in H^{r_1} \times \widehat{H}^{r_2}$ に対して、

$$\sigma(w) = \prod_{i=1}^{r_1+r_2} \sigma_i(w_i)$$

によって定義できる。

今、$x \in V$, $w = (w_1, \cdots, w_{r_1+r_2}) \in H^{r_1} \times \widehat{H}^{r_2}$ に対して、

$$\Phi(x) = \prod_{i=1}^{r_1+r_2} v_i^{\frac{1}{2}} \prod_{i=1}^{r_1} \exp(-\pi (x^{(i)})^2 v_i) \exp(\pi\sqrt{-1}\,(x^{(i)})^2 u_i) \prod_{i=r_1+1}^{r_1+r_2} \exp(-2\pi |x^{(i)}|^2 v_i)$$
$$\times \exp(\pi\sqrt{-1}\,((x^{(i)})^2 z_i + \overline{(x^{(i)})^2 z_i})$$

とする。ここで $1 \leqq i \leqq r_1$ に対して $w_i = (u_i, v_i)$, $r_1 + 1 \leqq i \leqq r_1 + r_2$ に対して $w_i = (z_i, v_i)$ である。そのとき、

$$\Phi^*(y) = \prod_{i=1}^{r_1} \left(\frac{v_i}{u_i^2 + v_i^2}\right)^{\frac{1}{2}} \prod_{i=r_1+1}^{r_1+r_2} \left(\frac{v_i}{|z_i|^2 + v_i^2}\right)^{\frac{1}{2}} \prod_{i=1}^{r_1} \exp\left(-\pi (y^{(i)})^2 \frac{v_i}{u_i^2 + v_i^2}\right)$$
$$\times \exp\left(\pi\sqrt{-1}\,(y^{(i)})^2 \frac{-u_i}{u_i^2 + v_i^2}\right) \prod_{i=r_1+1}^{r_1+r_2} \exp\left(-2\pi |y^{(i)}|^2 \frac{v_i}{|z_i|^2 + v_i^2}\right)$$
$$\times \exp\left(\pi\sqrt{-1}\left((y^{(i)})^2 \frac{-\bar{z}_i}{|z_i|^2 + v_i^2}) + \overline{(y^{(i)})^2} \frac{-z_i}{|z_i|^2 + v_i^2}\right)\right)$$

となる。そこで $\theta(w) = \sum_{m \in \mathfrak{G}} \Phi(m)$, $\omega = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ とおき、(5. 5) に今定義した $\Phi(x)$ とそれから得られた $\Phi^*(y)$ を代入すると

$$\theta(w) = \theta(\omega(w)) \tag{5. 8}$$

を得る。

次に $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の $\Gamma(4)$ の $\theta(w)$ への作用を考える。$c = 0$ のときは $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ の作用を考えればよいが、明らかに $\theta\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}(w)\right) = \theta(w)$ である。ゆえに $c \neq 0$ の場合を考えればよい。

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} \tag{5. 9}$$

となるので、$\theta(w)$ に $\begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$ を作用させて考察しよう。これは今やった議論と同じ事を

$$F(x) = \sum_{m \in \mathfrak{G}} e\left(\frac{c}{2d} m^2\right) \Phi(x + m) \tag{5. 10}$$

に対して行う。明らかに任意の $c \in d\mathfrak{G}$ に対して $F(x + c) = F(x)$ である。従ってフーリエの変換公式

$$\int_{(V/d\mathfrak{G})^* V/d\mathfrak{G}} F(x)\, e(xy)\, dx\, e(-yz)\, d^*y = F(z) \tag{5. 11}$$

を得る。前にやったのと同じようにして

$$\sum_{m\in\theta} e\left(\frac{c}{2d}m^2\right)\Phi(m) = |d|^{-\frac{1}{2}}Nd^{-1}\sum_{n\in\vartheta^{-1}}\left(\int_{V/d\theta}\sum_{m\in\theta} e\left(\frac{c}{2d}m^2\right)\Phi(x+m)\,e\left(x\cdot\frac{n}{d}\right)dx\right) \quad (5.12)$$

が得られる。$x+m=x'$ とおくと、

$$\int_{V/d\sigma}\sum_{m\in\sigma} e\left(\frac{c}{2d}m^2\right)\Phi(x+m)\,e\left(x\cdot\frac{n}{d}\right)dx$$

$$=\int_{V/d\sigma}\sum_{m\in\sigma} e\left(\frac{c}{2d}m^2\right)\Phi(x')\,e\left(-m\frac{n}{d}\right)e\left(x'\frac{n}{d}\right)dx'$$

$$=\int_{V}\sum_{u \bmod d} e\left(\frac{c}{2d}u^2\right)e\left(-\frac{un}{d}\right)\Phi(x')\,e\left(x'\frac{n}{r}\right)dx'$$

となる。

$$\sum_{u \bmod d} e\left(\frac{c}{2d}u^2\right)e\left(-\frac{un}{d}\right) = e\left(\frac{b}{2d}n^2\right)\sqrt{Nd}\left(\frac{2c}{a}\right) \quad (5.13)$$

に注意しながら、(5. 12) より

$$\sum_{m\in\sigma} e\left(\frac{c}{2d}m^2\right)\Phi(m) = |d|^{-\frac{1}{2}}Nd^{-1}\left(\frac{2c}{a}\right)\sqrt{Nd}\sum_{n\in\vartheta^{-1}} e\left(\frac{b}{2d}n^2\right)\Phi^*\left(\frac{n}{d}\right) \quad (5.14)$$

を得る。

また $\frac{c}{d}+w$ は $\begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$ によって $\frac{b}{d}+\omega(w')|_{w'=d^2w}$ にうつるので、(5. 14) から

$$\theta\left(\begin{pmatrix} b & -a \\ d & -c \end{pmatrix}(w)\right) = \left(\frac{2c}{a}\right)\theta(w) \quad (5.15)$$

が得られる。(5. 8) より $\theta(\omega(w))=\theta(w)$ であり、(5. 9) と (5. 15) より

$$\theta\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(w)\right) = \left(\frac{2c}{a}\right)\theta(w) \quad (5.16)$$

を得る。ところで、1）に関する事実より、もし (5. 2) における χ が $\Gamma(4)$ の指標ならば、平方剰余の相互法則が導き出されるはずであった。(5. 15) により、任意の $\sigma\in\Gamma(4)$ に対して

$$\theta(\sigma(w)) = \chi(\sigma)\,\theta(w)$$

である。これは χ が $\Gamma(4)$ の指標であることを言っているので、目標であった平方剰余の相互法則の証明が完成した。

5．3　ヒルベルトの第12問題と類体論

まずヒルベルトの第12問題の内容を述べることにする。それは次のようなものである。

第12問題：アーベル体に関するクロネッカーの定理を任意の代数体に拡張すること

というものである。この問題の源泉は明らかにクロネッカーであり、クロネッカーは1875年に次のことを証明した。

クロネッカーの定理：有理数体上のアーベル体はすべて円体である。

さらにクロネッカーは虚２次体上のアーベル体についてもデデキントにあてた手紙の中で予想を述べている。それは

予想：一般の虚２次体Kを取るとき、K上のアーベル方程式は、Kに所属する数を虚数乗法にもつ楕円関数の、Kの数に関する周期等分方程式と、そのような楕円関数の特異モジュラー方程式によって全て汲みつくされる

というものである。この予想はクロネッカーの青春の夢と名づけられ、1920年に日本の高木貞治が類体論を作りあげるとほぼ同時にその予想を解決した。この高木の活躍によって日本の数学は世界的なレベルに達し、類体論は日本の数学の中心としておかれることとなった。

ここで類体論というものをごく簡単に説明しておく。類体論とはアーベル拡大体論のことであり、ガウスを初めとする19世紀ドイツの数学の伝統を継いだもので、ヒルベルトによって概念的には確立された。kを基礎体とし、Kをそのアーベル拡大体としたとき、kのイデアルはKにおいて分解されることになる。その分解法則を述べたものが類体論である。さらに1927年のアルティンの相互律によって類体論は完成することになる。アルティンの相互律によってあらゆる巾剰余の相互法則が得られた。19世紀ドイツの整数論は巾剰余の相互法則をめざして発達してきたものであり、ヒルベルトを経て類体論というやや別の観点から巾剰余の相互法則は得られたのである。

クロネッカーに話をもどせば、クロネッカーはクロネッカーの定理とクロネッカーの青春の夢を語ると同時に、さらに壮大な夢を語っている。それは

夢：さらに進んで一般の複素数に対しても特異モジュールの類似物を見つけるという希望がある

というものである。これはまさにヒルベルトの第12問題に相当するもので19世紀ドイツの整数論の夢であった。

5．4　巾剰余の相互法則

5.3で述べたクロネッカーの青春の夢の中にでてきた虚数乗法という言葉を少し説明しよう。例えば、$a+bi$ (a, bは整数) を周期とする楕円関数（レムニスケート関数）を考える。この関数は$a+bi$を周期にもつが、虚数i倍してもまた周期になる。このように一般の楕円関数の周期に虚の代数的整数を乗ずることによって生じる現象を研究する理論を虚数乗法論という。

この虚数乗法論を押し進めていけば5.3で述べたヒルベルトの第12問題にぶつかるのであるが、この思想の根底にあるのは巾剰余の相互法則がある。しかし、現実には虚数乗法は類体論という本来の流れとは別の所から考察され、巾剰余の相互法則は類体論の一部であるアルティンの相互律から得られた。我々が言う本来の流れとは、5.2で述べた平方剰余の相互法則の証明の如くに任意の巾剰余の相互法則が得られることである。もしそれがかなうならばクロネッカーの夢の夢であるヒルベルトの第12問題も解決されることになるのであろう。

6．おわりに

数論における3大予想とクロネッカーの青春の夢という奇妙な取り合わせで書いてみたが、我々の感ずるところによれば、3大予想は巾剰余の相互法則にヒントがあると思われる。クロネッカーの青春の夢の奥底にあるのは巾剰余の相互法則であったから、このような取り合わせになった次第である。5.2で述べたスタイルで、巾剰余を越え、さら

に一般の相互法則の証明ができれば、3大予想に近づけるかもしれない。我々のめざす3大予想は形式的にはまったく異なる予想であるけれども、いつのひか相互法則が、それらを結びつけ新しい数学を産みだすことを、我々は真に願っている。

参考文献

1) T. Kubota, : Ein arithmetischer Satz uber eine Matrizengruppe, J. reine angew. Math., 222 (1966), 55-57.

2) 高瀬正仁：ガウスの遺産と継承者たち、海鳴社 (1990)

3) 藤崎源二郎、森田康夫、山本芳彦：数論への出発、日本評論社 (1980)