１００「フェルマーの最終定理（２）」その１　クンマーの証明

フェルマーの最終定理については、**博想録「４３」**で書いた。

「博想録」は一般に敬遠されがちな数学や物理学に関するテーマについて、解りやすく書くことを主眼としている。しかしフェルマーの最終定理については自分としては努力したつもりだが、まだまだ解りやすく書けているとは言えない。それは問題そのものが“超難解”ということもあるが、自分自身が充分に理解できていなかったことが一番の理由だ。そこで今回はさらによく理解するように努め、できるだけ多く例を盛り込んでより解りやすく書きたいと思う。

フェルマーの最終定理とは、表現のしかたはいくつかあるが、要するに
自然数 n≧3 に対して、$x^n + y^n = z^n$ を満たす自然数 $x,\ y,\ z$ は存在しないというものである。

問題の意味すら理解できないものが多い数学の難問にあって、このフェルマーの問題はシンプルで小学生でも理解できる。そして、何となく反例が見つかりそうな気もする。

最初のころは、３，４，５，７、、、、など、単独の数についての証明が行われた。すべての自然数は素数によって作られていることから、４以上の数については素数だけについて証明すればよいことになる。

しかし、無限に存在する素数を１１，１３，１７、、、、と一つずつ証明していたのでは埒が明かない。そんな中、フランスの女性数学者ソフィ・ジェルマンが１,８２３年、素数pで$2p+1$も素数の場合（例えば１１，２３，２９，４１，４３、、、など）について一般的な証明に成功した。このことは大いに評価されてよい。

素数を$p(primary\ number)$と表すと上式は、$x^p + y^p = z^p$ ----------①
と書ける。ドイツのクンマーは一般解を求めるため①の左辺を因数分解し、

$$x^p + y^p = (x+y)\left(x+\zeta_p^{\,1}y\right)\left(x+\zeta_p^{\,2}y\right)\left(x+\zeta_p^{\,3}y\right)\cdots\left(x+\zeta_p^{\,p-1}y\right) = z^p \quad \text{----------②}$$

とした。ここで、$\zeta_p^{\,1}$，$\zeta_p^{\,2}$，$\cdots\zeta_p^{\,p-1}$は１のp乗根、$\zeta_p^{\,n} = \cos(\frac{2\pi}{p}n) + \sqrt{-1}\sin(\frac{2\pi}{p}n)$と表され、

例えば $p=3$の場合、１の３乗根は1，$\zeta_3^{\,1} = \frac{-1+\sqrt{-3}}{2}$，$\zeta_3^{\,2} = \frac{-1-\sqrt{-3}}{2}$ である。

ここで、$\sqrt{-3}$は虚数、$\frac{-1+\sqrt{-3}}{2}$，$\frac{-1-\sqrt{-3}}{2}$は複素数である。

$$x^3 + y^3 = (x+y)\left(x+\frac{-1+\sqrt{-3}}{2}y\right)\left(x+\frac{-1-\sqrt{-3}}{2}y\right) = z^3 \quad \text{----------③}$$

と素因数分解され、
右辺がz^3なので、それぞれの（　）が互いに素であるとすると、素因数分解の一意性から

$(x+y)$，$\left(x+\frac{-1+\sqrt{-3}}{2}y\right)$，$\left(x+\frac{-1-\sqrt{-3}}{2}y\right)$ はそれぞれが３乗数でなくてはならない。

よって次のように書くことができる。

$x+y=(a_1+b_1\sqrt{-m_1})^3$，$x+\dfrac{-1+\sqrt{-3}}{2}y=(a_2+b_2\sqrt{-m_2})^3$，$x+\dfrac{-1-\sqrt{-3}}{2}y=(a_3+b_3\sqrt{-m_3})^3$

以上のことから（　）内のそれぞれが素であることを示し、上記を満たすa_1，a_2，a_3，b_1，b_2，b_3，m_1，m_2，m_3がないことを証明することにより、③を満たす自然数x，y，z がないことが証明される。(以下、証明は省略する)

さらに $p=5$の場合を示すと１の５乗根は、

1，$\zeta_5^{\,1}=\dfrac{-1+\sqrt{5}}{4}+\dfrac{\sqrt{-10-2\sqrt{5}}}{4}$，$\zeta_5^{\,2}=\left(\zeta_5^{\,1}\right)^2=\left(\dfrac{-1+\sqrt{5}}{4}+\dfrac{\sqrt{-10-2\sqrt{5}}}{4}\right)^2=\dfrac{-1-\sqrt{5}}{4}+\dfrac{\sqrt{-10+2\sqrt{5}}}{4}$,

$\zeta_5^{\,3}=\left(\zeta_5^{\,1}\right)^3=\left(\dfrac{-1+\sqrt{5}}{4}+\dfrac{\sqrt{-10-2\sqrt{5}}}{4}\right)^3=\dfrac{-1-\sqrt{5}}{4}-\dfrac{\sqrt{-10+2\sqrt{5}}}{4}$

$\zeta_5^{\,4}=\left(\zeta_5^{\,1}\right)^4=\left(\dfrac{-1+\sqrt{5}}{4}+\dfrac{\sqrt{-10-2\sqrt{5}}}{4}\right)^4=\dfrac{-1+\sqrt{5}}{4}-\dfrac{\sqrt{-10-2\sqrt{5}}}{4}$　となるので、

$$x^5+y^5=(x+y)\left[x+\left(\frac{-1+\sqrt{5}}{4}+\frac{\sqrt{-10-2\sqrt{5}}}{4}\right)y\right]\left[x+\left(\frac{-1-\sqrt{5}}{4}+\frac{\sqrt{-10+2\sqrt{5}}}{4}\right)y\right]$$
$$\left[x+\left(\frac{-1-\sqrt{5}}{4}-\frac{\sqrt{-10+2\sqrt{5}}}{4}\right)y\right]\left[x+\left(\frac{-1+\sqrt{5}}{4}-\frac{\sqrt{-10-2\sqrt{5}}}{4}\right)y\right]=z^5 \quad \text{----------④}$$

と素因数分解される。

以下 $p=3$の場合と同様、（　）内のそれぞれが素であり、かつ５乗数とならないことが言えればよい。（以下省略）

以上のことから、有理数体（整数，分数の集合）$\boldsymbol{Q}$ に$\zeta_p^{\,1}$，$\zeta_p^{\,2}$，$\cdots\cdot\zeta_p^{\,p-1}$を付加した$\boldsymbol{Q}(\zeta_p)$と表記される有理数の拡大体の中で素因数分解できれば、すべてのpに対して証明できると考えられる。(体とは数の集合であり、その集合内で＋－×÷の四則演算が自由にできるものと考えればよい)

ところが、クンマーはこの考え方は充分ではないことに気付く。

この証明で最も重要なことは、x^p+y^pを②式のように分解したとき、右辺の（　）内のそれぞれが互いに素であるという点である。

彼は $\boldsymbol{Q}(\zeta_p)$において、素因数分解の一意性が必ずしも成り立たない場合があることに気付いたのである。

例えば、整数の集合$\mathbf{Z}$に$\sqrt{-5}$を加えた拡大体$\mathbf{Z}\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}\middle|a,b\in\mathbf{Z}\right\}$の世界では６という整数は、$6=2\times3=\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$というように２通りに分解してしまい、素因数分解の一意性が成り立たない。$p=37$のときはより複雑である。

(1) $\boldsymbol{Q}(\sqrt{-1})$において、$37=(6+\sqrt{-1})(6-\sqrt{-1})$ ----------(ｲ)

(2) $\boldsymbol{Q}(\sqrt{3})$において、 $37=(7+2\sqrt{3})(7-2\sqrt{3})$ ----------(ﾛ)

(3) $\boldsymbol{Q}(\sqrt{-3})$において、$37=(5+2\sqrt{-3})(5-2\sqrt{-3})$ ----------(ﾊ) と分解される。

３７は$\boldsymbol{Q}(\zeta_{12})$ においてさらに多くの積に分解される。

ζ_pは図１に示す半径１の円において、円周のｐ等分点を複素数で表したもので円分体と言われる。

ζ_{12}では、$\zeta_{12}^{\,1}$, $\zeta_{12}^{\,2}$,$\cdots\cdot\zeta_{12}^{\,11}$は、ド・モアブルの公式 $cos\dfrac{2\pi n}{12}+\sqrt{-1}\,sin\dfrac{2\pi n}{12}$ において$n=1,\ 2,\ \cdots\cdot11$と

することにより得られる。
表１に示すように、$\boldsymbol{Q}(\zeta_{12})$ は$\sqrt{3}$，$\sqrt{-1}$，$\sqrt{-3}$ を含むので、
(4) $\boldsymbol{Q}(\zeta_{12})$において、

(ロ) は、$7+2\sqrt{3}=7+2\zeta_{12}^{1}+2\zeta_{12}^{11}$，　$7-2\sqrt{3}=7+2\zeta_{12}^{5}+2\zeta_{12}^{7}$

(ハ) は、$5+2\sqrt{-3}=5+2\zeta_{12}^{2}+2\zeta_{12}^{4}$，　$5-2\sqrt{-3}=5+2\zeta_{12}^{8}+2\zeta_{12}^{10}$

というように、それぞれ異なった２つの数の積に分解する。
さらに、$\boldsymbol{Q}(\sqrt[4]{-3},\ i)$においては次のように８つに分解してしまう。（ここでは$\sqrt{-1}=i$ と表記する）
(5) $\boldsymbol{Q}(\sqrt[4]{3},\ \sqrt{i})$において、

$\sqrt[4]{-3}=\sqrt{\sqrt{3}\,i}=\sqrt[4]{3}\sqrt{i}=\sqrt[4]{3}\left(\frac{1+i}{\sqrt{2}}\right)$，$\sqrt[4]{-3}^{3}=(\sqrt{\sqrt{3}\,i})^{3}=\sqrt[4]{3}^{3}\sqrt{i}^{3}=\sqrt[4]{3}^{3}\left(\frac{-1+i}{\sqrt{2}}\right)$ なので、

$$37=(\zeta_{12}^{4}+\boldsymbol{i}\sqrt[4]{-3}+\sqrt[4]{-3}^{3})(\zeta_{12}^{4}+\boldsymbol{i}\sqrt[4]{-3}-\sqrt[4]{-3}^{3})(\zeta_{12}^{4}-\boldsymbol{i}\sqrt[4]{-3}+\sqrt[4]{-3}^{3})(\zeta_{12}^{4}-\boldsymbol{i}\sqrt[4]{-3}-\sqrt[4]{-3}^{3}) \quad \text{---------(ニ)}$$

$$\times(\zeta_{12}^{8}+\boldsymbol{i}\sqrt[4]{-3}^{3}+\sqrt[4]{-3})(\zeta_{12}^{8}+\boldsymbol{i}\sqrt[4]{-3}^{3}-\sqrt[4]{-3})(\zeta_{12}^{8}-\boldsymbol{i}\sqrt[4]{-3}^{3}+\sqrt[4]{-3})(\zeta_{12}^{8}-\boldsymbol{i}\sqrt[4]{-3}^{3}-\sqrt[4]{-3}) \quad \text{---------(ホ)}$$

(ニ)を計算すると$-\frac{1}{2}-\sqrt{37-\frac{1}{4}}i$，(ホ)は$-\frac{1}{2}+\sqrt{37-\frac{1}{4}}i$ となり、これを掛けると３７になる。

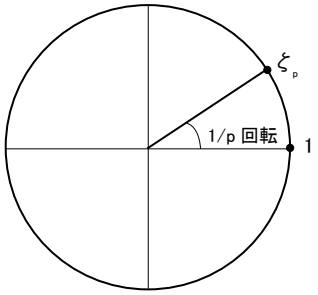


図1 複素平面における1のｐ乗根

円分体ζ_{12}の元	角度	1の12乗根の値	円分体ζ_{3}の元	円分体ζ_{4}の元
ζ_{12}^{0}	0	1	1	1
ζ_{12}^{1}	$\frac{\pi}{6}$	$\frac{\sqrt{3}}{2}+\frac{1}{2}i$		
ζ_{12}^{2}	$\frac{\pi}{3}$	$\frac{1}{2}+\frac{\sqrt{3}}{2}i$		
ζ_{12}^{3}	$\frac{\pi}{2}$	i		ζ_{4}^{1}
ζ_{12}^{4}	$\frac{2\pi}{3}$	$-\frac{1}{2}+\frac{\sqrt{3}}{2}i$	ζ_{3}^{1}	
ζ_{12}^{5}	$\frac{5\pi}{6}$	$-\frac{\sqrt{3}}{2}+\frac{1}{2}i$		
ζ_{12}^{6}	π	-1		ζ_{4}^{2}
ζ_{12}^{7}	$\frac{7\pi}{6}$	$-\frac{\sqrt{3}}{2}-\frac{1}{2}i$		
ζ_{12}^{8}	$\frac{4\pi}{3}$	$-\frac{1}{2}-\frac{\sqrt{3}}{2}i$	ζ_{3}^{2}	
ζ_{12}^{9}	$\frac{3\pi}{2}$	$-i$		ζ_{4}^{3}
ζ_{12}^{10}	$\frac{5\pi}{3}$	$\frac{1}{2}-\frac{\sqrt{3}}{2}i$		
ζ_{12}^{11}	$\frac{11\pi}{6}$	$\frac{\sqrt{3}}{2}-\frac{1}{2}i$		

表1 円分体ζ_{12}

このように$\boldsymbol{Q}\left(\zeta_{p}\right)$において素因数分解の一意性が成り立たない中、クンマーは素因数をより基本的な「素元数」に分解することで、素因数分解の一意性を成り立たせることが可能になると考え、これ以上分解できない数“理想数”の考え方を導入して、多くの素数について①の方程式に解がないことを証明し

た。これは、原子をさらに陽子と中性子に分解することに似てないだろうか？

理想数はその後、ドイツのデデキントにより抽象的概念を含めた“イデアル”として体系化され、新しい分野「代数的整数論」となって発展した。

イデアルをこれ以上分解できない素イデアルに分解することは、整数の素因数分解に対応した拡張概念で、代数体における素イデアル分解は整数の世界における素因数分解の一意性の一般化といえる。

クンマーはｐが５以上の素数で、

（１） x, y, zいずれもpで割れない場合

（２） x, y, zいずれかがpで割れる場合

に分けて考えた。ここでは、（１）のケースについて述べる。

有理数の集合である有理数体に、無理数や円分体を加えた$a_1 + b_1\sqrt{c_1}$，$a_2 + b_2\sqrt{c_2}$ $(a_1, a_2, b_1, b_2, c_1, c_2 \in \boldsymbol{Q})$，$\zeta_n$などを加えたものを代数体という。代数体には代数方程式の解となるすべての数（代数的数という）が含まれ、π や e といった代数方程式の解にならない数（超越数という）は含まれない。例えば、$\boldsymbol{Q}(\zeta_n)$は代数体である。

有理数体“$\boldsymbol{Q}$”の中に整数環（整数の集合で加，減と乗算について閉じている集合）があるように、代数体“$\boldsymbol{K}$”の中に $\boldsymbol{K}$ の整数環といわれる部分環 $\boldsymbol{O_k}$（代数体の整数環）を考えることができる。（図２）

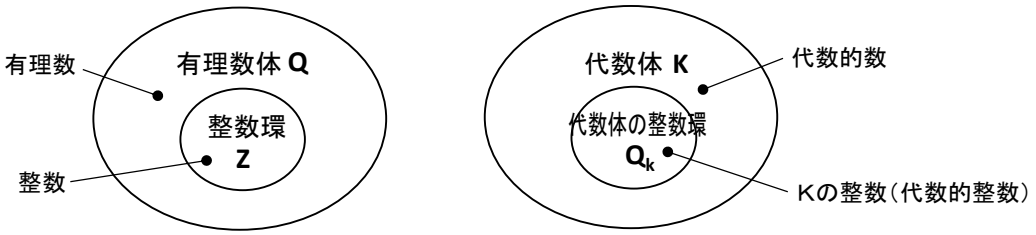


図２ 代数体の整数環

有理数体 $\boldsymbol{Q}$ は整数と分数の集合で、$\boldsymbol{Q}$ の元に対する四則演算（加，減，乗，除）の答えは必ず $\boldsymbol{Q}$ の中に存在する。例えば、$-\frac{1}{3}$，２に対する演算、$-\frac{1}{3}+2$，$-\frac{1}{3}-2$，$-\frac{1}{3}\times 2$，$-\frac{1}{3}\div 2$ の答え、$\frac{5}{3}$，$-\frac{7}{3}$，$-\frac{2}{3}$，$-\frac{1}{6}$はすべて $\boldsymbol{Q}$ に含まれている。つまり $\boldsymbol{Q}$ は四則演算が可能な集合で“体”と呼ばれる。（「四則演算に対して閉じている」という）一方、$\boldsymbol{Q}$ に含まれる整数の集合 $\mathbf{Z}$ は $\boldsymbol{Q}$ の部分集合で、加，減，乗算について閉じている。除算については必ずしも整数になるとは限らないので四則演算に対して閉じているとはいえず、このような集合を“環”と呼んでいる。“体”や“環”は代数構造といわれ、演算に応じた「単位元」「逆元」を持ち、結合法則や分配法則が成り立つ。

四則演算について閉じている有理数体 $\boldsymbol{Q}$ の中に、加，減，乗算に閉じている環という代数構造を持つ整数環 $\boldsymbol{Z}$ が存在する。これと同様に、四則演算について閉じている代数体 $\boldsymbol{K}$の中に、加，減，乗算に閉じている代数体の整数環体 $\boldsymbol{Q}$ の$\mathbf{O_k}$が存在するのである。

例えば、代数体$\boldsymbol{K} = \boldsymbol{Q}(\zeta_3)$において、$\zeta_3\left(-\frac{1}{2}+\frac{\sqrt{-3}}{2}\right)$と$\frac{1}{3}$に対する四則演算の結果、$-\frac{1}{6}+\frac{\sqrt{-3}}{2}$，

$-\frac{5}{6}+\frac{\sqrt{-3}}{2}$，$-\frac{1}{6}+\frac{\sqrt{-3}}{6}$，$-\frac{3}{2}+\frac{3\sqrt{-3}}{2}$は $\boldsymbol{K}$ に含まれている。

一方、代数体の整数環 $\boldsymbol{O_k} = \boldsymbol{Z}[\zeta_3]$の元$\zeta_3\left(-\frac{1}{2}+\frac{\sqrt{-3}}{2}\right)$と 3に対する加，減，乗算の結果、

$\frac{5}{2}+\frac{\sqrt{-3}}{2}$，　$-\frac{7}{2}+\frac{\sqrt{-3}}{2}$，　$-\frac{3}{2}+\frac{3\sqrt{-3}}{2}$ は $\boldsymbol{O_k}$に含まれ、除算の結果$-\frac{1}{6}+\frac{\sqrt{-3}}{6}$ は $\boldsymbol{O_k}$に含まれない。

$\boldsymbol{K=Q(\zeta_n)}$なら、$\boldsymbol{O_k=Z[\zeta_n]}=\left\{\sum_{i=0}^{r}a_i\,\zeta_n^{\,i}\ ;r\geqq 0,a_0,a_1,\cdots,a_r\in\boldsymbol{Z}\right\}$と表される。

代数体の整数環 $\boldsymbol{O_k}$ の元は、代数体 $\boldsymbol{K}$ の元 λ の中で $n\geqq 1$ と整数 $c_1,c_2,\cdots,c_n$ についてのn次方程式、$\lambda^n+c_1\lambda^{n-1}+c_2\lambda^{n-2}+\cdots+c_n=0$の式を満たすもの全体である。ここでのポイントは、この式の最高次λ^nの係数が 1 ということと、$c_1,c_2,\cdots,c_n$ が整数ということである。$\boldsymbol{O_k}$の元を$\boldsymbol{K}$ の整数（代数的整数）と呼ぶ。例えば、$\lambda^2-2\lambda+4=0$ の根である$\lambda_1=1+\sqrt{3}i$，$\lambda_2=1-\sqrt{3}i$ は $\boldsymbol{O_k}$ の元であり $\boldsymbol{K}$ の整数であるが、λ^2 の係数が 1 でない$2\lambda^2-2\lambda+1=0$ の根である$\lambda_1=\frac{1}{2}+\frac{1}{2}i$，$\lambda_2=\frac{1}{2}-\frac{1}{2}i$ は、$\boldsymbol{O_k}$ の元でなく$\boldsymbol{K}$ の整数ではない。

代数体の整数環においては、$\boldsymbol{Z}[\sqrt{2}]$，$\boldsymbol{Z}[\sqrt{-1}]$，$\boldsymbol{Z}[\zeta_3]$で成立した素元分解の一意性が成り立たないことがある。よく用いられる例であるが、$\boldsymbol{Q}(\sqrt{-5})$の整数環 $\boldsymbol{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\,;a,b\in\boldsymbol{Z}\}$ において、「６」は、$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$というように、２通りに分解される。$\boldsymbol{Z}[\sqrt{-5}]$において、「2」，「3」，「$1+\sqrt{-5}$」，「$1-\sqrt{-5}$」はこれ以上分解することはなく、いずれもそれぞれを割ることはない。

このように代数体の整数環 $\boldsymbol{Z}[\sqrt{-5}]$ では、6 の分解がただ一通とならない。しかし代数体の整数環においては、必ず素イデアル分解の一意性が成り立つ。

イデアルを（　）で表すものとし、分解したそれぞれのイデアルを(2)，(3)，$(1+\sqrt{-5})$，$(1-\sqrt{-5})$と表せば、$(2)=AB$，$(3)=CD$，$(1+\sqrt{-5})=AC$，$(1-\sqrt{-5})=BD$のように、素イデアルA，B，C，Dで表すことができる。これから、$(6)=(2)(3)=(1+\sqrt{-5})(1-\sqrt{-5})=ABCD$となり、$(6)=(AB)(CD)=(AC)(BD)=(ABCD)$と書け、４つの素イデアル$A$，$B$，$C$，$D$にただ一通りに分解されると考えることができる。

$\boldsymbol{K}$ を代数体、$\boldsymbol{\sigma}$ を$\boldsymbol{O_k}$ のイデアルとすると、$\boldsymbol{\sigma=p_1\cdot p_2\cdots p_r}$（$r\geqq 0$，$\boldsymbol{p_1,p_2,\cdots,p_r}$は $\boldsymbol{O_k}$ の素イデアル）のように素イデアルの積にただ一通りに分解される。（素イデアルはべき乗となることもある）

イデアルの定義は次のように示される。

代数体の整数環 $\boldsymbol{O_k}$ において、$\boldsymbol{O_k}$ の部分集合 $\boldsymbol{I}$ で、次の(ⅰ)(ⅱ)を満たすものを $\boldsymbol{O_k}$ のイデアルという。

(ⅰ) $a,b\in\boldsymbol{I}$ なら $a+b\in\boldsymbol{I}$，　$a-b\in\boldsymbol{I}$　(a,bが集合 I の元ならば、$a+b$，$a-b$も $\boldsymbol{I}$ の元である)

(ⅱ) $a\in\boldsymbol{I}$，　$x\in\boldsymbol{O_k}$ なら $ax\in\boldsymbol{I}$　　(aが $\boldsymbol{I}$ の元、xが整数環 $\boldsymbol{O_k}$ の元ならばaxは $\boldsymbol{I}$ の元である)

$\boldsymbol{O_k}$ の元である代数的整数 $\partial_1,\partial_2,\cdots,\partial_n$ と $\boldsymbol{O_k}$ の元 $x_1,x_2,\cdots,x_n$ で作られる$\{x_1\partial_1+x_2\partial_2+\cdots+x_n\partial_n\}$ は $\boldsymbol{I}$ のイデアルで、$\partial_1,\partial_2,\cdots,\partial_n$で生成される $\boldsymbol{O_k}$ のイデアルと呼び（$\partial_1,\partial_2,\cdots,\partial_n$）と書き、$(\partial_1,\partial_2,\cdots,\partial_n)=\{x_1\partial_1+x_2\partial_2+\cdots+x_n\partial_n\}$を表す。

$\boldsymbol{O_k}$ のただ１つの元 ∂ により生成されたイデアル $(\partial)=\{\partial x\}$を単項イデアル（または主イデアル）という。$\boldsymbol{O_k}$ のイデアル $\boldsymbol{p}$ が素イデアルとは、

(ⅰ) $a,b\in\boldsymbol{O_k}$ かつ $ab\in\boldsymbol{p}$ なら $a\in\boldsymbol{p}$
　　または$b\in\boldsymbol{p}$

(ⅱ) $1\notin\boldsymbol{I}$（これは $\boldsymbol{p}\neq\boldsymbol{O_k}$ ということ）

という条件を満たすことをいう。

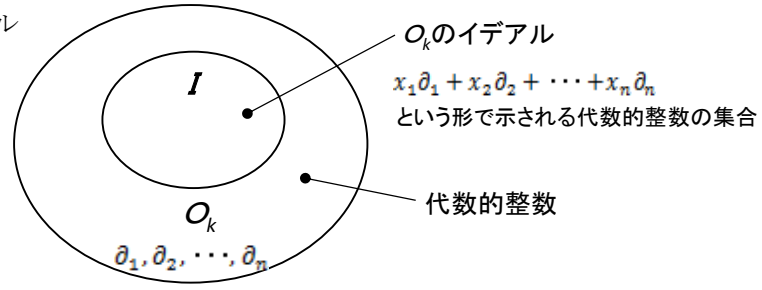


図３　代数体の整数環

イデアルどおしの掛け算は、$(a_1,a_2)(b_1,b_2)=(a_1b_1,a_1b_2,a_2b_1,a_2b_2)$となる。
イデアル(a,b)は、$x_1,x_2\in \boldsymbol{O_k}$とすると $(a,b)=\{ax_1+bx_2\}$と表せ、a,bの最小公倍数を c とすると、ユークリッドの互除法により、$ax_1+bx_2=cx$となるので、$(a,b)=\{ax_1+bx_2\}=\{cx\}$ のように単項イデアルとなる。

また、単項イデアル(a)，(b) が $(a)=(b)$であるとき、 $a=\varepsilon b$ が成り立つ。
ここで、ε は単数である。単数とは共通の約数と考えればよく、整数の世界では±1、複素数の世界では±1，$\pm\sqrt{-1}$ であり、代数体の世界、例えば $\boldsymbol{Q}(\sqrt{2})$で 7 は、$7=(3+\sqrt{2})(3-\sqrt{2})=(5+3\sqrt{2})(5-3\sqrt{2})$ などと２つの数の積で表せるが、$3+\sqrt{2}=(1+\sqrt{2})^2(5-3\sqrt{2})$ となるので、$3+\sqrt{2}$は $5-3\sqrt{2}$から $(1+\sqrt{2})^2$を使って生成されることがわかる。

このとき$1+\sqrt{2}$ を $\boldsymbol{Q}(\sqrt{2})$ の単数という。

分数イデアルとは、$\boldsymbol{O_k}$ のイデアル$(a,b)=\{ax_1+bx_2\}=\{cx\}$に対し、
$\boldsymbol{O_k}$ のもとの体 $\boldsymbol{K}$ に属する元 φ(ここで φ は分数とする)により生成されるイデアル$\{\ \varphi cx\}$である。

さて、ここでどうしても触れておかなければならないのが「イデアル類群」である。
代数体 $\boldsymbol{K}$ のイデアル類群 Cl_k とは、

$$Cl_k=\frac{\boldsymbol{O_k}\text{の分数イデアル全体が乗法についてなす群}}{\boldsymbol{O_k}\text{の単項イデアル全体のなす群}}$$

と定義される。

代数的整数論は、より広い概念である代数体を対象とし、その整数環を考え整数全体を外側から眺めることによって整数の性質を理解しようとする。代数体の整数環においては、素因数分解の一意性を成り立たせるためイデアルを考えるが、最終的に知りたいのは整数の性質である。そのためイデアルと整数の性質がどれくらいズレているかを知るためにイデアル類群を考えるのである。

$\boldsymbol{O_k}$ の２つのイデアル$\boldsymbol{p_1}$，$\boldsymbol{p_2}$ に対し、$\boldsymbol{K}$ の０でない元φで$\boldsymbol{p_1}=\varphi\boldsymbol{p_2}$ となるものが存在するとき、$\boldsymbol{p_1}$と$\boldsymbol{p_2}$は同じ類に属するものとして分類する。これらの類をイデアル類と呼び有限個であり，その数を類数という。イデアル類を扱いやすい群として把えるため、整数環 $\boldsymbol{O_k}$ のイデアルの集合を一般化し分数イデアルにするのである。

整数 $\boldsymbol{Z}$ においてイデアルは倍数の集合で、例えば偶数は“２”で生成される単項イデアルということができる。$\boldsymbol{Z}$ を群として把えようとすると、逆元が存在しなければならないので分数が必要となり、整数でなく分数を含む有理数に拡張して把えることになる。$\boldsymbol{O_k}$ においても、同様の考え方で分数イデアルを含めた集合に拡張したのである。

$\boldsymbol{O_k}$ の分数イデアル全体の集合を $\boldsymbol{I_k}$ とすると、この集合においては積に対して結合法則，交換法則が成り立ち単位元が存在し、任意の元に対して逆元が存在する。従って $\boldsymbol{I_k}$ は可換群である。

さらに単項イデアル全体の集合を $\boldsymbol{P_k}$ とすると、$\boldsymbol{P_k}$ は $\boldsymbol{I_k}$ の部分群であり、可換群の任意の部分群は正規部分群であるから、$\boldsymbol{P_k}$ と $\boldsymbol{I_k}$ の間に剰余群（商群）$Cl_k=\frac{\boldsymbol{I_k}}{\boldsymbol{P_k}}$ を考えることができ、これがイデアル類群そのものである。

単項イデアルとは $\boldsymbol{K}^{\times}$（$\boldsymbol{K}$ の可逆元全体のなす乗法群；ここで乗法群とは乗法に対して結合法則，分配法則が成り立ち乗法に対する逆元を持つ群をいう）の元 β により生成される(β)----$\{\beta \in \boldsymbol{K}^{\times}\}$という形の分数イデアルである。

$\boldsymbol{K}^{\times}$ は体 $\boldsymbol{K}$ の元の中で乗法についての逆元を持つ元（可逆元という）全体のなす乗法群を表す。（ただし 0 を除く）例えば、整数を 8 で割った余りの数による集合（剰余類という）

$\mathbf{Z}_8 = [\mathbf{Z}/8\mathbf{Z}] = \{0,1,2,3,4,5,6,7(mod8)\}$ について考えてみる。

$\mathbf{Z}_8$ の中ですべての掛け算を行うと表２のとおりとなり、$\mathbf{Z}_8$ は積に対する単位元「1」、0 でない他の元に積の逆元（表２において「$1\times1=1$」，「$3\times3=9=1(mod8)$」，「$5\times5=25=1(mod8)$」，「$7\times7=49=1(mod8)$」）が存在するので体である。

従って、$\mathbf{Z}_8$ の逆元の集合 $\mathbf{Z}_8^{\times}$ は乗法について体をなし、その元は 8 と素な数によってつくられ、$\mathbf{Z}_8^{\times} = [\mathbf{Z}/8\mathbf{Z}]^{\times} = \{1,3,5,7\}$ である。

$\mathbf{Z}_8^{\times}$ の中での掛け算は表３のようになる。

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

表2 $\mathbf{Z}_8$ における掛け算

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

表3 $\mathbf{Z}_8^{\times}$ における掛け算

イデアル類群とは具体的にどのようなものなのか？

例えば $\boldsymbol{K} = \boldsymbol{Q}(\zeta_{23})$ を考えてみる。この代数体の類数は３なので、

イデアル類群 Cl_k は３次の巡回群になり、

$Cl_k = \frac{\boldsymbol{I_k}}{\boldsymbol{P_k}} = \{\ \boldsymbol{P_k}, \boldsymbol{pP_k}, \boldsymbol{p^2P_k}\}$ と表わされる。ここで $\boldsymbol{p}$ は単項分数イデアルでない分数イデアルである。単項イデアルの集合 $\boldsymbol{P_k}$ に属する分数イデアルは、$\boldsymbol{p}$ を掛けると $\boldsymbol{pP_k}$に属する分数イデアルになり、 $\boldsymbol{pP_k}$に属する分数イデアルは、$\boldsymbol{p}$ を掛けると $\boldsymbol{p^2P_k}$ に属する分数イデアルになる。（図４）

さらに $\boldsymbol{p^2P_k}$に属する分数イデアルに $\boldsymbol{p}$ を掛けると単項分数イデアルに戻る。すなわちイデアル類群は、それぞれの分数イデアルが単項分数イデアルからどれくらい離れているかを表している群ということができる。

代数体 $\boldsymbol{K}$ のイデアル類群 Cl_k の元の数がその代数体の類数であるが、クンマーは $\boldsymbol{Q}(\zeta_p)$の類数が p で割れないという仮定のもとで、

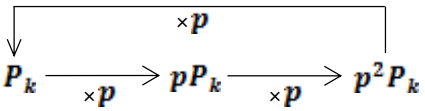


図4 ３次の巡回群となる
$\boldsymbol{K} = \boldsymbol{Q}(\zeta_{23})$ のイデアル類群の関係

x，y，zいずれもpで割れないケースに対して証明した。

②により、

$x^p + y^p$ は $\boldsymbol{O_k} = \boldsymbol{Z}[\zeta_p]$ の中で、$(x+y)\left(x+\zeta_p^{1}y\right)\left(x+\zeta_p^{2}y\right)\cdots\cdots\left(x+\zeta_p^{p-1}y\right) = z^p$ と分解される。

右辺 z^pはイデアル(z)の $\boldsymbol{p}$ 乗と表せるので、

$$(x+y)\left(x+\zeta_p^{1}y\right)\left(x+\zeta_p^{2}y\right)\cdots\cdots\left(x+\zeta_p^{p-1}y\right) = (z)^p \quad \text{----------⑥}$$

⑥の右辺に対し $\boldsymbol{O_k}$ の可逆元 εと $\boldsymbol{O_k}$ の元 $\boldsymbol{a}$ の間に、

$$
\left.
\begin{array}{l}
x+y=\varepsilon_0{\alpha_0}^p \\
x+\zeta_p^{\,1}y=\varepsilon_1{\alpha_1}^p \\
\quad\text{----------} \\
x+\zeta_p^{\,p-1}y=\varepsilon_{p-1}{\alpha_{p-1}}^p
\end{array}
\right\} ⑦
$$

を満たすものが存在することを証明する。

まず、⑥の左辺（　　）内のイデアル $x+\zeta_p^{\,i}y\ (0\le i\le p-1)$は、すべてお互いに素であることを示す。

$0\le i\le j\le p-1$とし、$\boldsymbol{\alpha}$を$(x+\zeta_p^{\,i}y)$と$(x+\zeta_p^{\,j}y)$ ともに割り切る $\boldsymbol{O_k}$ の 0 でない素イデアルとする。

$x+\zeta_p^{\,i}y,\ x+\zeta_p^{\,j}y\in\boldsymbol{\alpha}$より、$\left(\zeta_p^{\,i}-\zeta_p^{\,j}\right)x,\ \left(\zeta_p^{\,i}-\zeta_p^{\,j}\right)y\in\boldsymbol{\alpha}$であるから、$\zeta_p^{\,i}\left(1-\zeta_p^{\,j-i}\right)(x,y)\in\boldsymbol{\alpha}$

となる。 x,yは互いに素であるから、$(x,y)=(1)$である。

$1\le i\le p-1$に対し、$\left(1-\zeta_p^{\,1}\right)=(1-\zeta_p^{\,i})$から、$(1-\zeta_p^{\,j-i})=(1-\zeta_p^{\,1})$ となるので、

$\boldsymbol{O_k}$において$(1-\zeta_p^{\,1})$ は素イデアルである。従って、$\boldsymbol{O_k}$における$(\boldsymbol{\alpha})$の素イデアル分解は、

$(\boldsymbol{\alpha})=(1-\zeta_p^{\,1})^{p-1}$である。⑥より$z^p\in\boldsymbol{\alpha}$、よって$z\in\boldsymbol{\alpha}$となる。

$\boldsymbol{\alpha}$と$\boldsymbol{Z}$の共通、$\boldsymbol{\alpha}\cap\boldsymbol{Z}=(a)$ だから z は pで整除され、x,y,z がいずれもpで割り切らないという仮定に反する。従って、イデアル$x+\zeta_p^{\,i}y$ は $\boldsymbol{O_k}$ のあるイデアルの p 乗となる。

よって⑦が証明された。

⑦の一般項をi とすると、$x+\zeta_p^{\,i}y=\varepsilon_i{\alpha_i}^p$ と表せる。イデアル類群の元はフェルマーの小定理 (※1)

により、イデアル類群の類数乗すると単位元に戻る。これは、類数 3 の $\boldsymbol{K}=\boldsymbol{Q}\left(\zeta_{23}\right)$ の場合について図４に示したとおりである。イデアル類群の類数をh 、単項イデアルα_i の属する類を $\boldsymbol{P_i}$ とすると、

${\alpha_i}^h=\boldsymbol{P_i}$

また、α_i はp 乗すると $\boldsymbol{P_i}$ になるから ${\alpha_i}^p=\boldsymbol{P_i}$ である。ここで h とp が互いに素ならば、この２つの整数の間にはユークリッドの互除法により、$ha+pb=1$となる整数 $a,\ b$ が存在する。

よって、${\alpha_i}^{ha+pb}=\alpha_i$ が成り立つので、α_i が単項イデアルであることが証明された。

以上より、p がイデアル類群の類数を割り切らないならば①が成り立つ。

イデアル類群の類数を割り切らない素数を「正則素数」という。一方、割り切る素数を「非正則素数」といい、非正則素数についてはこれまで述べてきたクンマーの方法では①が証明されない。

正則素数か非正則素数かは、円分体 $\boldsymbol{Q}(\zeta_p)$の類数を調べることによってわかる。

１００までの素数のうち非正則素数は表４に示す３つのみである。非正則素数の類数を素因数分解すると、因数にかならず自分自身が含まれ類数を割り切ることがわかる。

p	類 数	類数の素因数分解
37	37	<u>37</u>
59	41241	3×<u>59</u>×233
67	853513	<u>67</u>×12739

表4 非正則素数

$\boldsymbol{\alpha}$の生成元をαとすると、$\left(x+\zeta_p^{\,1}y\right)\cdot\alpha^{-p}\in \boldsymbol{O_k}^{\times}$である。

$\boldsymbol{O_k}^{\times}$は$\boldsymbol{O_k}$の可逆元全体のなす乗法群で、$\left(x+\zeta_p^{\,1}y\right)\cdot\alpha^{-p}$が$\boldsymbol{O_k}^{\times}$の元であることを示している。

（※１）フェルマーの小定理

「pを素数とし、pと互いに素な整数aに対して、$a^{p-1}\equiv 1(mod\ p)$が成り立つ。」

この定理は、aの$p-1$乗をpで割った余りは 1 であるというもので、ある数が素数でないことを、実際に素因数分解することなく判定できる。

例えば、$3^{20}(mod\ p)$を計算する場合、$3^{20}=3^{6\cdot3+2}=3^{6\cdot3}\cdot3^2=(3^6)^3\cdot3^2$、ここで定理$3^{7-1}\equiv 1(mod\ 7)$を用いると、$(3^6)^3\cdot3^2\equiv 1^3\cdot3^2\equiv 9\equiv 2(mod\ 7)$から、$3^{20}\equiv 2(mod\ 7)$となることがわかる。

「フェルマーの最終定理（２）」その２　アンドリュー・ワイルズの証明

代数学的手法を拡張したクンマーの方法により、正則素数については証明されたが、非正則素数については証明されない。正則素数同様非正則素数も無限に存在するので、これでは証明したことにならない。この問題が完全に証明されたのは、クンマーから１００年以上経過した後のことだった。

「４３」ではわかりにくかった、アンドリュー・ワイルズによる証明の部分について、私のできる範囲で分かりやすく書いていきたいと思う。「４３」とあわせて読んでいただきたい。

これから、本論ともいうべきその方法について書いていく。

まず、フェルマーの定理、$x^n + y^n = z^n \ (n \geq 3)$ を証明するための道筋についてまとめておく。

（道筋を示すため用語や記号の説明は省略、後に【　　】で示される）

１．方程式 「$x^n + y^n = z^n$」 に解があったと仮定してその矛盾を導く

２． 両辺を z^n で割って、$\left[\frac{x}{z}\right]^n + \left[\frac{y}{z}\right]^n = 1$ とし、$\frac{x}{z} = X$, $\frac{y}{z} = Y$ とおくと、$X^n + Y^n = 1$ となる

$x,\ y,\ z$ は自然数だから $\frac{x}{z}$, $\frac{y}{z}$ は有理数（分数や小数）である。よって、問題は $X^n + Y^n = 1$ を満たす有理数 $X,\ Y$ を求める問題となる。

３． $X^n + Y^n = 1$ において、この曲線の複雑さは n によって決まる。n は種数といい、$n = 3$ のときは楕円曲線である。$n \geq 3$ のとき、モーデル・ファルティングスの定理により、有理点は有限個であることが証明されている。この定理から、$X^n + Y^n = 1$ に解があるとすれば、その解は有限個である。そこで“楕円曲線の有理点は有限個しかない”という性質を利用して証明していく。

４．谷山・志村予想「有理数体上の楕円曲線のゼータ関数は、上半平面上の重み２の、ある保型形式のゼータ関数に一致する」により、楕円曲線から導かれるゼータ関数と保型形式から導かれるゼータ関数を突き詰めていけば証明できるはずである。

５．楕円曲線と保型形式を同じ土俵で論ずるため「ガロア表現」【ガロア群を行列の形で表したもの】を使う。

６．楕円曲線からガロア表現を導くために、楕円曲線が群構造を持つことを利用する。

楕円曲線の n 等分点の群 $\mathrm{E}[n]$ から得られるガロア群から、ベクトル空間への写像により行列の形で表したガロア表現を導く。ここで、群 $\mathrm{E}[n]$ はアーベル群（可換群）であり、剰余類を $\boldsymbol{Z}/n$ と表せば $\boldsymbol{Z}/n \oplus \boldsymbol{Z}/n$ に同型である。

有理数体 $\boldsymbol{Q}$ の代数的閉包（$\boldsymbol{Q}$ 上のすべての有限次ガロア拡大を含む体）を $\overline{\boldsymbol{Q}}$ で表し、その絶対ガロア群を $G_{\boldsymbol{Q}} = Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ とする。このとき、$G_{\boldsymbol{Q}}$ のベクトル空間への連続的な作用として得られる準同型写像をガロア表現という。この場合のガロア表現は $GL_2(\boldsymbol{Z}/n)$ と表され２次正則行列全体である。

7．p を素数、n を正の整数としたとき、楕円曲線の p^n 等分点の群 $\mathrm{E}[p^n]$ を考える。その p 倍写像 $\mathrm{E}[p^{n+1}] \to \mathrm{E}[p^n]$ に関する逆極限を $T_p(\mathrm{E})$ とすると、$T_p(\mathrm{E}) = \varprojlim \mathrm{E}[p^n]$ をテイト加群といい、階数２の自由 $\boldsymbol{Z_p}$ 加群である。 $T_p(\mathrm{E})$ にガロア群 G_Q を作用させると、連続な準同型写像 $\rho_p : G_Q \to GL_2(\boldsymbol{Z_p})$ が得られる。

8．準同型写像 ρ_p の核 $Ker\,\rho_p$ に対応する拡大を $\boldsymbol{K_p\infty/G_Q}$ とする。すなわち $Gal(\overline{\boldsymbol{Q}}/\boldsymbol{K_p\infty}) = Ker\,\rho_p$ である。l を素数（$l \neq p$）、Ｅは l で良い還元を持つとし、$Frob_l$ を l におけるフロベニウス共役類とすると、$det\left(\boldsymbol{\rho}_p(Frob_l)\right) = l$ が成り立つ。また $\boldsymbol{\rho}_p(Frob_l)$ のトレースは、$Tr\left(\boldsymbol{\rho}_p(Frob_l)\right) = \boldsymbol{a}_l$ となる。

ここで、有限体 $\boldsymbol{F_l}$ におけるＥの有理点全体の数を $\sharp\, E(F_l)$ とすると、$\sharp\, E(F_l) = l + 1 - \boldsymbol{a}_l$ が成り立つ。つまり、楕円曲線を有限体 $\boldsymbol{F_l}$ の世界で方程式として解いたときの解の個数が、ガロア群の作用から得られることを示している。

9．楕円曲線Ｅのディリクレ Ｌ関数を $\mathrm{L}(\mathrm{E},\mathrm{s})$ と表し、次の式で定義する。

$$\mathrm{L}(\mathrm{E},\mathrm{s}) = \prod_{\text{よい素数}} (1 - a_l l^{-s} + l^{1-2s})^{-1} \times \prod_{\text{よくない素数}} (1 - a_l l^{-s})^{-1}$$

Ｌ関数はＥの各素数 l における情報を貼り合わせて作られ、このＬ関数を通して見ることによりＥの性質がわかる。ディリクレＬ関数の特別な場合が楕円曲線のゼータ関数であり、この中に $\boldsymbol{a}_l$ が現れる。

１０．$\boldsymbol{Q}$ 上の楕円曲線Ｅに対して、導手と呼ばれる正の整数Ｎが定義される。導手は、Ｅが良い還元を持たないような素数（悪い素数）すべての積である。
$q = e^{2\pi iz}$ とし、変数 q に関するべき級数展開したとき、$\boldsymbol{a}_l$ を q^l の係数に持つ、重さ２，レベルＮのヘッケ作用素の同時固有関数 $\sum \boldsymbol{a_n}\, q^n$ が存在する。

１１．ヘッケ作用素の同時固有関数 $\sum \boldsymbol{a_n}\, q^n$ において、 $\boldsymbol{a_1 = 1}$ の場合をカスプ形式という。このカスプ形式 $f = \sum \boldsymbol{a_n}\, q^n$ に対して、$\boldsymbol{K = Q}_p(\boldsymbol{a_n})$ とおくと、$\boldsymbol{K/Q}_p$ は有限次拡大であり、連続な既約表現

$\rho_f : G_Q = Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q}) \to GL_2(\boldsymbol{K})$ で、$Tr\left(\boldsymbol{\rho}_f(Frob_l)\right) = \boldsymbol{a}_l$，$det\left(\boldsymbol{\rho}_f(Frob_l)\right) = l$ を満たすものが存在する。これで、楕円曲線の「ガロア表現 ρ_p」と保型形式の「ガロア表現 ρ_f」が導かれ、谷山・志村予想「Ｅを $\boldsymbol{Q}$ 上に定義された導手Ｎの楕円曲線とするとき、そのＬ関数から導かれるゼータ関数は、重み２，レベルＮの保型形式のゼータ関数に一致する。」が具体的に結びついた。

１２．Ｅを $\boldsymbol{Q}$ 上に定義された導手Ｎの楕円曲線とし、$\mathrm{L}(\mathrm{E},\mathrm{s})$ をディリクレ級数の形 $\mathrm{L}(\mathrm{E},\mathrm{s}) = \sum_{n=1}^{\infty} \frac{\boldsymbol{a_n}}{n^s}$ と書くと、$\boldsymbol{a_n}$ は a_lに一致する。このとき、$f = \sum_{n=1}^{\infty} \boldsymbol{a_n} q^n$ は重さ２，レベルＮの保型形式である。

１３．上記で得られた重さ２，レベルＮの保型形式が実際には存在しないことを示し矛盾を導く。

ここで、非常に特殊な楕円曲線であるフライの考えた曲線 $E_n : y^2 = x(x+a^n)(x-b^n)$ を導入する。

フライ曲線の判別式は、$D = [a^n b^n (a^n + b^n)]^2 = (abc)^{2n}$ であり、このフライ曲線 E_n は判別式が自然数の $2n$ 乗数であり、位数２の点を持ちしかも半安定である。しかし、このような曲線は保型形式の理論からは存在しないので矛盾する。

１４．ワイルズは、有限体 $\boldsymbol{F_3}$ から得られる既約表現 $G_Q = GL_2(\boldsymbol{F_3})$ がモジュラーであり、既に証明されていることを使い、標数 $\boldsymbol{p}$ の有限体において、 $G_Q = GL_2(\boldsymbol{F})$ は保型形式から得られることにたどり着いた。最終的にワイルズは、ガロア表現から来る変形環Ｒと、保型形式から来るヘッケ環Ｔの間の準同型写像 $\varphi : R \to T$ が同型写像（Ｒ＝Ｔ）であることを証明し、フェルマー予想の証明に成功した。
（Ｒ＝Ｔの証明については、私の力では理解困難であり岩波講座「現代数学の展開 Fermat 予想１」をそのまま引用する）

ここから本論に入る。

ゲルハルト・フライにより示された特殊な楕円曲線（フライ曲線）から導かれたゼータ関数は、谷山・志村予想【「すべての楕円曲線はモジュラーである」という予想で“楕円曲線”と“保型形式”がうまく対応するというもの】により、重さ２，レベル２の保型形式になる。よってこのフライ曲線からは、重さが２でレベルが２の保型形式が存在しなければならないことになる。

しかし、保型形式の理論によれば、そのような関数は存在しないことがわかっているので、谷山・志村予想が正しければフェルマー予想も正しいことになるのである。

従って、**「すべての楕円曲線はモジュラーである」**(※1) ということを証明すればフェルマー予想が証明される。ただし、この場合の楕円曲線は、係数が有理数かつ準安定な楕円曲線【素数を法としその方程式を解いたとき、重根は持っても三重根を持たない楕円曲線】であることが条件である。

楕円曲線と保型形式を同じ土俵で論ずるため「ガロア表現」【ガロア群を行列の形で表したもの】を使う。楕円曲線は群構造を持っていること、つまり演算できることが大きな特徴であるが、群は抽象的でわかりにくいので、ベクトル空間 【和と積が定義されている空間】への写像により行列の形にすることで解りやすくしたものが“表現”である。

楕円曲線から導かれるガロア表現【楕円曲線から得られるガロア群からベクトル空間への写像でガロア群を行列の形で表現したもの】と保型形式から導かれるガロア表現を比較する。

以下、$\mathbf{N}$：自然数の集合，$\mathbf{Z}$：整数の集合，$\mathbf{Q}$：有理数の集合，$\mathbf{R}$：実数の集合，$\mathbf{C}$：複素数の集合，
p：素数　を表すものとする。

谷山－志村予想を具体的に書くと、

『**有理数体 $\boldsymbol{Q}$ 上の楕円曲線Ｅ**(※2)（Elliptic curve）と、**正規化された同時固有カスプ形式**(※3)

$$\boldsymbol{f}(z) = \sum_{n=1}^{\infty} a_n q^n \qquad \cdots\cdots\cdots\cdots\cdots\cdots ①$$

において、ほとんどすべての素数p【重根とならないpでよい還元をもつ素数をいう】に対して、
$a_p(E) = a_p(f)$ を満たすものが存在する』ということができる。ここで、
$a_p(E)$は、楕円曲線Ｅを$mod\ p$で解いた時の解の個数N_pから$a_p(E) = p - N_p$として求められる。
$a_p(f)$は、①を展開したときにあらわれる係数a_nの中で順番が素数である項にあらわれる係数である。
このような式が成り立つということは本当に驚くべきことで、全く不思議としか言いようがない。
このあたりの詳細は**博想録「７２」**３７２～３７８ページを参照していただきたい。

これを証明するために、**楕円曲線Ｅのn等分点**(※4)の群 Ｅ$[n]$ から導かれるガロア群をもとに、ベクトル空間への写像を行列の形で表したガロア表現を導く。有理数体$\boldsymbol{Q}$の代数的閉包（$\boldsymbol{Q}$上のすべての有限次ガロア拡大を含む体）を$\overline{\boldsymbol{Q}}$で表し、その絶対ガロア群を$G_{\boldsymbol{Q}} = Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$とするとき、$G_{\boldsymbol{Q}}$のベクトル空間への連続的な作用として得られる準同型写像がガロア表現である。

ここで、有理数体$\boldsymbol{Q}$上の楕円曲線Ｅとは、
整数$\boldsymbol{Q}$の世界で考える（yの２次式）＝（xの３次式)という形をした方程式で、
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (係数a_iは整数) と表され、変数変換を行うことにより次のような一般形で書くことができる。

Ｅ：$y^2 = x^3 + ax + b \quad (a, b \in \boldsymbol{Q})$　　……②　（重根を持たないものだけを楕円曲線という）

次に、楕円曲線の有理点を調べるため、楕円曲線Ｅを有限体$\boldsymbol{F_p}$上で考える。
有限体$\boldsymbol{F_p}$は、整数を素数pで割った余りの数による集合（剰余類）で$\boldsymbol{Z/pZ}$と表す。

例えば$\boldsymbol{F_{23}}$は$\{0,1,2,3\cdots\cdots22\}$という２３個の数からなる体で、この中で楕円曲線を描くと離散した点となる。有限体$\boldsymbol{F_p}$（p=2,3,5,7……)上で方程式Ｅ：$y^2 = x^3 - x$を解いた時の解の個数は次の表１のようになる。

$\boldsymbol{F_p}$	$\boldsymbol{F_2}$	$\boldsymbol{F_3}$	$\boldsymbol{F_5}$	$\boldsymbol{F_7}$	$\boldsymbol{F_{11}}$	$\boldsymbol{F_{13}}$	$\boldsymbol{F_{17}}$	$\boldsymbol{F_{19}}$	$\boldsymbol{F_{23}}$	・・・・・・・・・
個数	2	3	7	7	11	7	15	19	23	・・・・・・・・・

（表１ 有限体$\boldsymbol{F_p}$での$y^2 = x^3 - x$の解の個数）

楕円曲線の各素数pについて$\boldsymbol{F_p}$での解の様子がわかれば、その楕円曲線の有理点の様子がわかる。
有理数体に対して絶対ガロア群を考えたが、同様に任意の体に対して絶対ガロア群を考えることができる。$\boldsymbol{F_p}$上で考えることで、有限体$\boldsymbol{F_p}$の絶対ガロア群は、有限体の最も特徴的な性質の１つである、フロベニウス写像と呼ばれる特別な元により（位相的に）生成されるアーベル群となる。

$\boldsymbol{F_p}$上の楕円曲線Ｅは、**幾何的フロベニウスと呼ばれる自己準同型**(※5)【$g(x\cdot y) = g(x)\cdot g(y)$ あるいは、$g(x+y) = g(x) + g(y)$ が成り立つとき g を準同型写像という】をもつ。 フロベニウス写像の特別な性質を利用することで、代数体【有理数体の拡大体】がフロベニウス写像と同型になりその形が把握できるのである。

幾何的フロベニウスとは、Ｅの座標の元をすべてp乗することによって定まるＥの自己準同型$(x, y) \rightarrow (x^p, y^p)$で定義される代数体の写像である。

$\boldsymbol{F_p}$において$\boldsymbol{F_p}$の全ての元xはフェルマーの小定理【素数pと互いに素な整数aに対して$a^p - 1 \equiv 1(mod\ p)$が成り立つ】により$x^p = x$を満たす。従って$\boldsymbol{F_p}$の元は方程式$x^p - x = 0$のp個の根（元）を決定し、どんなに体を拡大しても根の数はp個より多くの根を持つことはない。

特に体が $\boldsymbol{F_p}$ の代数拡大体【すべての代数的数を付加した拡大体で代数的閉包という】であれば、その代数拡大体のフロベニウス写像に関する不変体は $\boldsymbol{F_p}$ である。

楕円曲線Ｅを p を法として還元【$\boldsymbol{F_p}$ の世界で方程式を解くこと】して得られる $\boldsymbol{F_p}$ 係数の方程式【$\boldsymbol{F_p}$ 上の楕円曲線】を $\boldsymbol{E_{F_p}}$とすると、有理数体 $\boldsymbol{Q}$ 上の楕円曲線Ｅを$mod\ p$ で解いた時の解の個数 N_p から、$a_p = p - N_p$として求めた a_p は、$\boldsymbol{E_{F_p}}$の$\boldsymbol{F_p}$ 有理点の集合
$\boldsymbol{E_{F_p}(F_p)} = \{(x,y) \in \boldsymbol{F_p} \times \boldsymbol{F_p} \mid y^2 = x^3 + ax + b\}$ = 元の個数　から、$a_p(E) = p + 1 -$ (元の個数) として求めることができる。

代数体 $\boldsymbol{K}$ において $\boldsymbol{K} = \boldsymbol{F_p}$ としたとき、各自然数 n ごとに $\boldsymbol{K}$ の n 次拡大がただ一つ存在して、それは $\boldsymbol{F_p}$ のフロベニウス写像 $\boldsymbol{F_{p^n}}$ と同型である。有限体の拡大のガロア群は、フロベニウス自己同型の繰り返しにより生成されるので $\boldsymbol{F_{p^n}}$ を考えておけば、ガロア群がすべて分かることになる。

次に $\boldsymbol{Q}$ 上の**楕円曲線Ｅの解（元）が群構造をなす**(※6)ことを述べる。図１において、楕円曲線Ｅ上の点 α，β をとり、その２点を通る直線とＥとの交点を$\gamma'(x,y)$とする。つまり、α，β，γ' は同一線上にある。

このことを、加法の記号＋を用いて $\alpha + \beta + \gamma' = 0$ と表すものとする。この式が成り立つように、２点 α，β の間の加法を導入する。

０は単位元であり、楕円曲線が②式で表されている時は無限遠点である。$\alpha + \beta + \gamma' = 0$ を変形して、$\alpha + \beta = 0 - \gamma'$ とすると、０は単位元だから、$0 = \gamma' - \gamma'$ として入れると、$\alpha + \beta = (\gamma' - \gamma') - \gamma'$ より、
$\alpha + \beta = -\gamma'$ となる。Ｅは x 軸に対して対称だから、$\gamma\,(x,-y)$ が $-\gamma'$ となり、$\alpha + \beta = \gamma$ が導かれる。

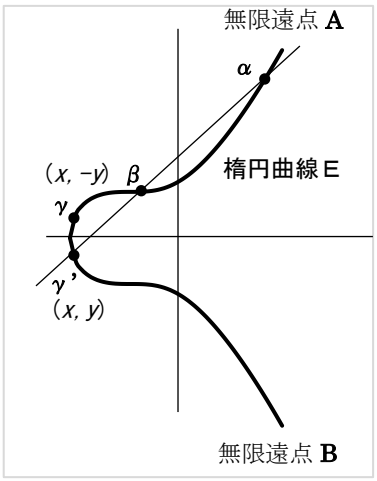


図１　Ｑ上の楕円曲線

このように加法演算が定義でき、γ は元の座標（α,β の座標）の有理式で表せる。さらに $\gamma + \gamma' = 0$ となり、$\gamma' = -\gamma$ （逆元がある）
$\alpha + \beta = \beta + \alpha$（交換法則）及び $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$（結合法則）が成り立つ。$x - y$ 平面で無限遠点を０とみなし、それを加法の単位元とすれば、楕円曲線Ｅ上の点は群構造を持つとみなせる。
無限遠点Ａと無限遠点Ｂはつながっているものと考える。

Ｅ上の点Ｐにおいて、ある自然数 n についてのＰの n 倍 (nP) が０となるＰのことを楕円曲線の等分点という。また n を固定したとき、nP が０となるＰを n 等分点という。

n 等分点全体はＥ($\boldsymbol{Q}$)の部分群でありn^2 個の元をもち、しかもある n 等分点 A，Bをうまくとると、すべての n 等分点は $aA + bB$ の形にただ一通りに表せる。例えば $E : y^2 = x^3 + 1$ について、複素領域で考えた場合の３等分点について具体的に考えてみる。

３等分点なので、$3P = 0$ を満たす。これを変形すると$2P = -P$ となり、これは両辺の x 座標が等しいということを表している。**楕円曲線の加法公式．２倍公式**(※7) により、

$P = (x,y)$とすると，$2P$ の x 座標は$\dfrac{x^4 - 8x}{4(x^3 + 1)}$、これが x に等しいので、$\dfrac{x^4 - 8x}{4(x^3 + 1)} = x$

これを計算して $x(x^3 + 4) = 0$ を得る。この式を満たす x は、$x = 0$，$x = -\sqrt[3]{4}$，$-\sqrt[3]{4}\omega$，$-\sqrt[3]{4}\omega^2$ である。ここで、$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ を表す。

よって３等分点の座標は、$(0,\pm1)$，$\left(-\sqrt[3]{4},\pm\sqrt{3}i\right)$，$\left(-\sqrt[3]{4}\omega,\pm\sqrt{3}i\right)$，$\left(-\sqrt[3]{4}\omega^2,\pm\sqrt{3}i\right)$ の８個に、無限遠点を加えた９個（3^2個）であり、$Z_3\times Z_3$ の構造となっている。すべての等分点は $aA+bB$ の形で表され、３等分点では $0\leqq a<3$，$0\leqq b<3$ である。以上をまとめると表２のようになる。

	0	1	2
0	0	$(-\sqrt[3]{4},\sqrt{3}i)$	$(-\sqrt[3]{4},-\sqrt{3}i)$
1	$(0,1)$	$(-\sqrt[3]{4}\omega,\sqrt{3}i)$	$(-\sqrt[3]{4}\omega,-\sqrt{3}i)$
2	$(0,-1)$	$(-\sqrt[3]{4}\omega^2,\sqrt{3}i)$	$(-\sqrt[3]{4}\omega^2,-\sqrt{3}i)$

表２　３等分点の座標

次の式で表される複素数 s の正則関数の無限積を、楕円曲線Ｅのディリクレ Ｌ関数といい $\mathrm{L}(\mathrm{E},\mathrm{s})$ と書く。Ｌ関数はＥの各素数 p における情報を貼り合わせて作られ、このＬ関数を通して見ることによりＥの性質がわかる。

$$\mathrm{L}(\mathrm{E},\mathrm{s})=\prod_{\text{よい素数}}(1-a_p(E)\bar{p}^{s}+p^{1-2s})^{-1}\times\prod_{\text{よくない素数}}(1-a_p(E)\bar{p}^{s})^{-1}\qquad\cdots\cdots\cdots\cdots③$$

ここで「よい素数」とは、$\boldsymbol{F_p}$ 上で $y^2=f(x)$ を解いたとき重根を持たない素数、「よくない素数」とは重根を持つ素数をいう。

なぜここでＬ関数が出てくるのかというと、ディリクレＬ関数の特別な場合が楕円曲線のゼータ関数であり、そのゼータ関数は保型形式と繋がっているからである。

次に、複素数体 $\boldsymbol{C}$ 上で楕円曲線Ｅを考える。

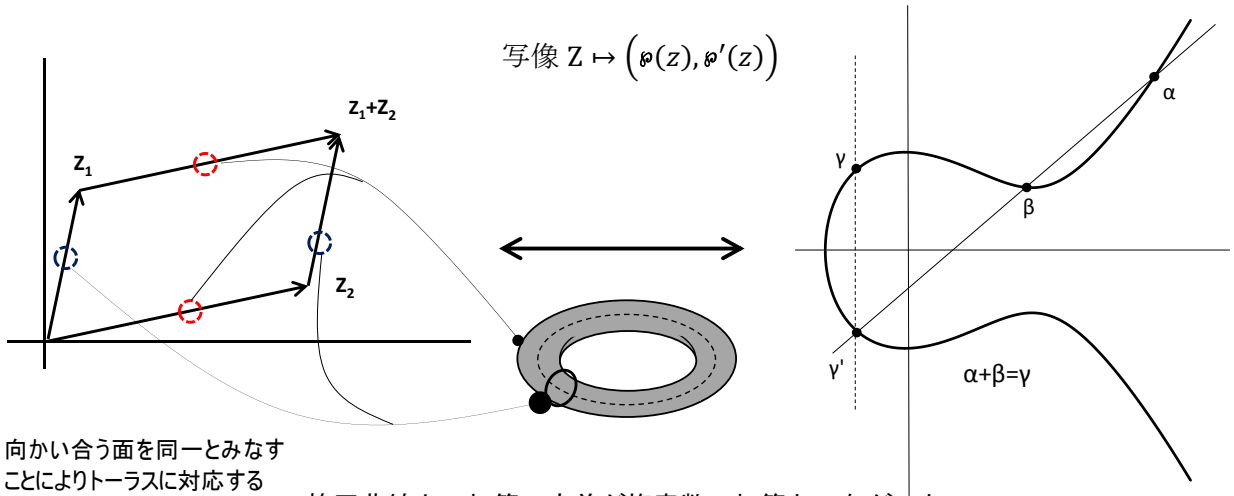
その理由は、楕円曲線Ｅがこの後に述べる複素平面上で定義するワイエルシュトラスの楕円関数（$\wp$ 関数：ペー関数）を通してモジュラー関数と繋がっており、複素数体（$\boldsymbol{C}$）における n 等分点が有理数体（$\boldsymbol{Q}$）におけるフロベニウス同型写像に対応するからである。

楕円曲線Ｅの複素数解はトーラス【ドーナツ型の図形】になる。

複素数体上の楕円曲線(※8) は、後述するように Ｅ：$y^2=4x^3-g_2x-g_3$ の形に変形できる。

複素平面 $\boldsymbol{C}$ において、実部と虚部がともに整数である複素数全体の集合をＬ（Lattice）とする。

Ｌは整数 $\boldsymbol{Z}$ とそれぞれ独立に動く複素数の組 $(\omega_1,\ \omega_2)$ をとり、格子 $\mathrm{L}=\mathrm{Z}\omega_1+\mathrm{Z}\omega_2$のように表される



楕円曲線上の加算の定義が複素数の加算とつながった

図２　複素トーラスと楕円曲線のつながり

複素トーラス $\boldsymbol{C}/\mathrm{L}$を考えることができる。

この $\boldsymbol{C}/\mathrm{L}$が ワイエルストラスの $\wp$ 関数呼ばれる関数を使って、楕円曲線上の点と１対１に対応する

ことが次のように示される。

℘関数は、$\boldsymbol{C}$ 内の格子Ｌを決めるごとに決まる複素変数関数 ℘(z) で次の式で定義される。

$$\wp(z) = \frac{1}{z^2} + \sum_{w\epsilon L\neq\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right) \qquad \cdots\cdots\cdots\cdots ④$$

$\wp(z)$ は $\boldsymbol{C}$ 上の有理型関数で、格子Ｌの点に２つの極を持つほかは正則である。またこの関数はＬの任意の元 $w\epsilon$Ｌ に対し $\wp(z + w) = \wp(z)$ を満たすので、二重周期を持つことがわかる。

$\wp(z)$を微分して$\wp'(z)$ をつくると、

$$\wp'(z) = -2\sum_{w\epsilon L} \frac{1}{(z-w)^3}$$

g_2，g_3 を、$g_2 = 60 \sum_{w\epsilon L\neq\{0\}} \frac{1}{w^4}$ ……⑤

$$g_3 = 140 \sum_{w\epsilon L\neq\{0\}} \frac{1}{w^6} \qquad \cdots\cdots\cdots\cdots ⑥$$

とすると、

$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ ……⑦ が成り立つ。

写像 $Z \to (\wp(z),\ \wp'(z))$ を考えると、上式からこの写像は、

$y^2 = 4x^3 - g_2x - g_3$ への写像となることがわかる。

$\wp(z)$，$\wp'(z)$ は二重周期をもつので、この写像は$\boldsymbol{C}/$Ｌ からの写像をひきおこし、$\boldsymbol{C}/$Ｌ から曲線

Ｅ：$\{(x,y)\epsilon\, \boldsymbol{C}^2 |\ y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$ への１対１の写像となる。このようにして℘関数から楕円曲線が導かれる。よって複素トーラス $\boldsymbol{C}/$Ｌと楕円曲線Ｅを同一視することができ、$\boldsymbol{C}$ が持つ加法群の構造がＥに移植され、それを具体的に記述するのが℘関数の加法公式ということになる。

２種類の格子 L_1，L_2 の作る複素トーラス $\boldsymbol{C}/\mathrm{L}_1$，$\boldsymbol{C}/\mathrm{L}_2$ が同型であるのは、L_1 と L_2 が定数倍、つまり $\mathrm{L}_1 = \alpha\mathrm{L}_2$ となる $\alpha \in \boldsymbol{C}^{\times}$（$\boldsymbol{C}$ の 0 以外の元全体のなす乗法群）が存在するときに限る。$\mathrm{L} \to \alpha\mathrm{L}$ とすると⑤，⑥式より、$g_2(\alpha\mathrm{L}) = \alpha^{-4}\, g_2(\mathrm{L})$，$g_3(\alpha\mathrm{L}) = \alpha^{-6}\, g_3(\mathrm{L})$ となるので曲線の方程式は変わる。

しかしαのべき乗が打ち消しあうような、例えば $g_2(\mathrm{L})^3 / g_3(\mathrm{L})^2$ を考えると、$\mathrm{L} \to \alpha\mathrm{L}$で不変となって複素トーラス（楕円曲線）は同型になるのである。ただし、$g_3(\mathrm{L})^2$が 0 にならないために、楕円曲線の判別式が 0 とならないことが条件である。

n を正の整数とするとき、群 $\boldsymbol{C}/$Ｌ の中で n 倍して消える元全体【n 等分点といい n 乗根の核を表す】、$\mathrm{E}[n] = \{x \in \boldsymbol{C}/\mathrm{L}\ ;nx = 0\}$ は、$\boldsymbol{Z}/n \oplus \boldsymbol{Z}/n$【$\boldsymbol{Z}/n$ は n で割った余り p が等しい整数をすべて集めたもので剰余類といい、$\boldsymbol{Z}/n\boldsymbol{Z}$，あるいは $\boldsymbol{Z_n}$ と書く。n が n_1，n_2 のとき $\boldsymbol{Z}/n_1 \oplus \boldsymbol{Z}/n_2 = \boldsymbol{Z}/(n_1 + n_2)$ となる】に同型である。このことは、複素数体 $\boldsymbol{C}$ における n 倍が有理数体 $\boldsymbol{Q}$ におけるフロベニウス同型写像に対応していることを示していると考えることができる。

有理数体 $\boldsymbol{Q}$ の代数的閉包を $\overline{\boldsymbol{Q}}$ で表し、その絶対ガロア群を $G_{\boldsymbol{Q}} = \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$と表す。

代数的閉包は、$\boldsymbol{Q}$ の最大の代数拡大（前出）であり代数的数体ともいう。

有理数体 $\boldsymbol{Q}$ の絶対ガロア群とは何か？

絶対ガロア群は、すべての代数的拡大体を含む巨大な群であり、ガロア群は自己同型群の中で特別なも

のである。

自己同型とは、群の代数的構造を保ちながら対象をそれ自身へと写像する方法のことで、その対象の対称性を表わしていると言うことができる。対象の全ての自己同型写像の集合は群をなし、それを自己同型群という。群Gの自己同型写像全体を $Aut(\boldsymbol{G})$ とすると、$\boldsymbol{G}$ の元を何度合成しても$\boldsymbol{G}$ に移されるので $Aut(\boldsymbol{G})$ は写像の合成に関して閉じていると言える。同型写像なので逆写像もあり、逆写像を逆元，恒等写像を単位元と考えれば自己同型写像の全体はやはり群の構造を持つと考えられ、これも自己同型群と考えられる。ガロア群は写像を元とする群ということができる。

体として有理数体 $\boldsymbol{Q}$ を考えたとき、$\boldsymbol{Q}$ を $\boldsymbol{Q}$ に写す自己同型写像は恒等写像【完全に１対１の対応となる写像】のみである。$\boldsymbol{Q}$ に無理数を付加した拡大体、例えば$\sqrt{2}$ を加えた $\boldsymbol{Q}(\sqrt{2})$ の場合、$\boldsymbol{Q}(\sqrt{2})$ の元は全て $\boldsymbol{a}+\boldsymbol{b}\sqrt{2}:a,b\in\boldsymbol{Q}$ という形であらわされ、$\boldsymbol{Q}(\sqrt{2})$を $\boldsymbol{Q}(\sqrt{2})$ に写す自己同型写像は２つあり、

Ｉ：$(\boldsymbol{a}+\boldsymbol{b}\sqrt{2})\to(\boldsymbol{a}+\boldsymbol{b}\sqrt{2})$という写像（恒等写像）と、Ｊ：$(\boldsymbol{a}+\boldsymbol{b}\sqrt{2})\to(\boldsymbol{a}-\boldsymbol{b}\sqrt{2})$ という写像（共役写像）【$(\boldsymbol{a}+\boldsymbol{b}\sqrt{2})$を$(\boldsymbol{a}-\boldsymbol{b}\sqrt{2})$ に$(\boldsymbol{a}-\boldsymbol{b}\sqrt{2})$を$(\boldsymbol{a}+\boldsymbol{b}\sqrt{2})$ に移す写像】がある。

体 $\boldsymbol{K}$ について、$\boldsymbol{K}$ から$\boldsymbol{K}$ への自己同型写像全体を $Aut(\boldsymbol{K})$とすると、これらは写像の合成に関して群を構成し、体 $\boldsymbol{K}$ の自己同型群と呼ぶ。

体の自己同型写像は、体から体への１対１の写像で加減乗除の演算を保つ写像である。

$\boldsymbol{L}$ を体 $\boldsymbol{K}$ の拡大体とし、その体の拡大を $\boldsymbol{L}/\boldsymbol{K}$ と表わすとき、$\boldsymbol{L}/\boldsymbol{K}$に対して体 $\boldsymbol{K}$ の自己同型写像全体 $Aut(\boldsymbol{K})$ の元 σ について，任意の $\boldsymbol{L}$ の元 $\boldsymbol{x}$ に対して $\sigma(x)=x$ となるもの（拡大体 $\boldsymbol{L}$ において $\boldsymbol{K}$ の元を動かさない自己同型写像）全体を $Aut(\boldsymbol{L}/\boldsymbol{K})$ と書く。$Aut(\boldsymbol{L}/\boldsymbol{K})$ は $Aut(\boldsymbol{K})$ の部分群となり、$Aut(\boldsymbol{L}/\boldsymbol{K})$ の元の個数が体の拡大次数に等しい場合がガロア群で、体 $\boldsymbol{K}$ の $\boldsymbol{L}$ 上のガロア群と呼ぶ。

例えば、$\boldsymbol{K}=\boldsymbol{Q}$，$\boldsymbol{L}=\boldsymbol{Q}(\sqrt{2})$ とすると、$Aut(\boldsymbol{L}/\boldsymbol{K})$ の元の個数は恒等写像Ｉと共役写像Ｊという２つの元のみであり、$\boldsymbol{L}$ の任意の元を $x_1=a_1+b_1\sqrt{2}$,$x_2=a_2+b_2\sqrt{2}$ としたとき、これらの２つの元に対して、加減乗除のいずれの計算をしても、結果は必ず $\boldsymbol{a}+\boldsymbol{b}\sqrt{2}$ という結果になるので拡大次数は２である。

従って[元の個数]＝[体の拡大次数]となるので $Aut(\boldsymbol{L}/\boldsymbol{K})$ はガロア群であり、それを$Gal(\boldsymbol{L}/\boldsymbol{K})$ と書く。

また、$\boldsymbol{K}=\boldsymbol{R}$ (実数体)，$\boldsymbol{L}=\boldsymbol{C}$ (複素数体) とすると、$[\boldsymbol{L}:\boldsymbol{K}]=2$，$Aut(\boldsymbol{L}/\boldsymbol{K})=\{\sigma_1,\sigma_2\}$,

σ_1 は恒等写像，σ_2 は複素共役写像である。従って$\boldsymbol{C}$は$\boldsymbol{R}$ のガロア拡大であり、$Gal(\boldsymbol{C}/\boldsymbol{R})\cong\boldsymbol{Z}/2\boldsymbol{Z}$ となる。

さらに、$\boldsymbol{K}=\boldsymbol{Q}$，$\boldsymbol{L}=\boldsymbol{Q}(\sqrt{2},\sqrt{3})$ とすると、$[\boldsymbol{L}:\boldsymbol{K}]=4$，$Gal(\boldsymbol{L}/\boldsymbol{K})=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ となる。

ここでσ_1は恒等写像，σ_2，σ_3，σ_4 はそれぞれ、

$\sigma_2(\sqrt{2})=\sqrt{2}$，$\sigma_2(\sqrt{3})=-\sqrt{3}$，　（$\sqrt{2}$ を変えず $\sqrt{3}$ は $-\sqrt{3}$ に）

$\sigma_3(\sqrt{2})=-\sqrt{2}$，$\sigma_3(\sqrt{3})=\sqrt{3}$，　（$\sqrt{3}$ を変えず $\sqrt{2}$ は $-\sqrt{2}$ に）

$\sigma_4(\sqrt{2})=-\sqrt{2}$，$\sigma_4(\sqrt{3})=-\sqrt{3}$　（$\sqrt{2}$ を $-\sqrt{2}$ に，$\sqrt{3}$ を $-\sqrt{3}$に）する写像である。

$\boldsymbol{Q}(\sqrt{2},\sqrt{3})$ の元は、$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ という形で書ける。

$\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$，$\sigma_2{}^2=\sigma_2(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6})=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=\sigma_1$

$\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$，$\sigma_3{}^2=\sigma_3(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6})=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=\sigma_1$

$\sigma_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$，$\sigma_4{}^2=\sigma_4(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=\sigma_1$

となるので、$\sigma_2{}^2=\sigma_3{}^2=\sigma_4{}^2=\sigma_1=1$ である。

$\sigma_2\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=\sigma_3\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=(a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6})=\sigma_4$、

よって、$\boldsymbol{L}$ は $\boldsymbol{K}$ のガロア拡大であり、ガロア群の構造は、

$Gal(\boldsymbol{L}/\boldsymbol{K})\cong\boldsymbol{Z}/2\boldsymbol{Z}\otimes\boldsymbol{Z}/2\boldsymbol{Z}$ である。

つまりガロア群は $\boldsymbol{L/K}$ の自己同型写像の特別な場合の集合で、写像の合成を演算とする群であり、拡大体 $\boldsymbol{L}$ が代数的閉包の場合が絶対ガロア群である。

楕円曲線上の点 $\mathrm{P}=(x,y)\in \mathrm{E}(\mathbf{C})$, $n\mathrm{P}=0$ とするとき、この点 $\mathrm{P}=(x,y)$ に対してガロア群の元 $\sigma=\boldsymbol{G_Q}$ （絶対ガロア群）の作用を $\sigma(\mathrm{P})=(\sigma(x),\sigma(y))$ と定義する。
$\mathrm{P}\in \mathrm{E}[n]$ となる P は、e_1,e_2 を基底とすると $\mathrm{P}=ae_1+be_2,\ a,b\in \boldsymbol{Z}/n$ と表せる。$n\mathrm{P}=0$ であれば、$n\sigma(\mathrm{P})=\sigma(n\mathrm{P})=0$ だから $\sigma(\mathrm{P})$ も $\mathrm{E}[n]$ に属す。そこで、$\sigma(e_1)=ae_1+ce_2,\ \sigma(e_2)=be_1+de_2$ とすれば、σ の n 倍して消える点への作用は行列として表すことができ、$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2(\boldsymbol{Z}/n)$ と書くことができる。ここで $GL_2(\boldsymbol{Z}/n)$ は剰余類 $\boldsymbol{Z}/n$ 上の２次正則行列全体を表す。

このようにして群の準同型写像、$\boldsymbol{\rho}_{\mathrm{E}[n]}$; $G_{\boldsymbol{Q}}\to GL_2(\boldsymbol{Z}/n)\qquad \sigma\to\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ が定義される。

$\mathrm{E}[p^n]$ を楕円曲線Eの p^n 等分点のなす群とする。
p^n 等分点 $\mathrm{E}[p^n]$ の p 倍写像、$\mathrm{E}[p^{n+1}]\to\ \mathrm{E}[p^n]$ に関する逆極限を $T_{\boldsymbol{p}}(\mathrm{E})$ とすると、
$\cdots\cdots \xrightarrow{\times n} \mathrm{E}[p^{n+1}]\xrightarrow{\times n}\mathrm{E}[p^n]\xrightarrow{\times n}\cdots\cdots\cdots\xrightarrow{\times n}\mathrm{E}[p^2]\xrightarrow{\times n}\mathrm{E}[p]$
$T_{\boldsymbol{p}}(\mathrm{E})=\varprojlim \mathrm{E}[p^n]$（射影極限）をテイト加群という。
$\mathrm{E}[p^n]\cong \boldsymbol{Z}/p^n\boldsymbol{Z}\oplus\boldsymbol{Z}/p^n\boldsymbol{Z}$ であり、その逆極限だから $T_{\boldsymbol{p}}(\mathrm{E})\cong \boldsymbol{Z}p\oplus\boldsymbol{Z}p$ となり、
$T_{\boldsymbol{p}}(\mathrm{E})$ は階級２の $\boldsymbol{Z}p$ 自由加群である。テイト加群 $T_{\boldsymbol{p}}(\mathrm{E})$ には絶対ガロア群
$G_{\boldsymbol{Q}}=Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ が連続かつ線形に作用する。
加群は加法に関して可換な群で、自由加群とは加法群で基底を持つものである。基底はその群の基準となるもので、階級２は基底の数が２であることを示し、その群の元はすべて基底の線型結合として表される。
e_1,e_2 を $T_{\boldsymbol{p}}(\mathrm{E})$ の $\boldsymbol{Z_p}$ 加群に対する基底とし、$\sigma(e_1)=ae_1+ce_2,\quad \sigma(e_2)=be_1+de_2$ とすると、
$\boldsymbol{\rho}(\sigma)=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2(\boldsymbol{Z_p})$ と定義することにより、連続な準同型写像

$\boldsymbol{\rho}_p$: $G_{\boldsymbol{Q}}\to\ GL_2(\boldsymbol{Z}_p)$ が得られる。この準同型写像は $\mathbf{E}[p^n]$ への作用
$\boldsymbol{\rho}_{\mathrm{E}[p^n]}$: $G_{\boldsymbol{Q}}\to\ GL_2(\boldsymbol{Z}/p^n)$ の逆極限として捉えることもできる。

このとき有限体上の方程式の解の個数と、このガロア群の作用との間に次の定理がある。
（定 理）
準同型写像 $\boldsymbol{\rho}_p$: $G_{\boldsymbol{Q}}\to\ GL_2(\boldsymbol{Z}_p)$ の核 $Ker\,\boldsymbol{\rho}_p$ に対応する拡大を $K_{p^\infty}/\boldsymbol{Q}$ $\left[Gal(\overline{\boldsymbol{Q}}/K_{p^\infty})=Ker\,\boldsymbol{\rho}_p\right]$ とする。
l はEでよい還元をもつ素数とし、$l\neq p$ とする。このとき、l は $K_{p^\infty}/\boldsymbol{Q}$ で不分岐【$\boldsymbol{Q}$ の拡大体K_{p^∞} において素イデアルに分解しない】であり、$Frob_l$ をl でのフロベニウス共役類とすると、

$det\left(\boldsymbol{\rho}_p(Frob_l)\right)=l$【$l$ でのフロベニウス共役類の作る写像の正方行列の行列式】が成り立つ。

従って$det(\boldsymbol{\rho}_p)$ は円分指標($\kappa: Gal(\boldsymbol{Q}(\mu_{p^\infty})/\boldsymbol{Q})\ \to\ \boldsymbol{Z}_p^{\times}$)に一致する。

また、$Tr\left(\boldsymbol{\rho}_p(Frob_l)\right)=a_l$ とおくと a_l は整数であり、$\#\,E(F_l)=l+1-a_l$ となる。

ここで、Tr は l でのフロベニウス共役類の作るトレース【行列の主対角成分の総和】、$E(F_l)$ は E の F_l 有理点全体【方程式の F_l での解と原点とでなす群】であり、$\sharp\, E(F_l)$ は［方程式の解の個数］+1 である。

このようにして方程式の解の個数がガロア群の作用から得られ、有限体の拡大についてのガロア群と同型になるという不思議な結びつきの事実が得られる。

また、$Tr\left(\boldsymbol{\rho}_p(Frob_l)\right)$ つまり a_l は p によらず決まることもわかる。

以上から、楕円曲線Ｅにおいて非常に重要な意味を持つ数列 $(a_l)_l$ の存在が明らかとなる。

$\boldsymbol{Q}$上の楕円曲線Ｅの a_l に対して q 展開の係数に同じ a_l を持つ**保型形式**（※9）が存在する。

$$\sum a_n q^n \qquad \cdots\cdots\cdots\cdots\cdots\cdots ⑧$$

q 展開とは、$q = e^{2\pi iz}$ とおいたときの変数 q についてのべき級数展開をいう。
z は複素上半平面、$\mathrm{H} = \{z \in \mathbf{C} | Im(z) > 0\}$ の変数で $q = e^{2\pi iz}$ より $|q| \leq 1$ のとき級数は絶対収束する。

$\boldsymbol{Q}$ 上の楕円曲線Ｅに対して、**導手**(※10)と呼ばれる正の整数 N が定義される。
導手は、楕円曲線のディリクレＬ関数の性質に深く関わっており、非常に重要である。

導手は、Ｅがよい還元をもたないような素数すべての積である。 Ｎを割り切るかどうかで素数が二分され、割り切るものを“悪い素数”、割り切らないものを“良い素数”という。

このとき、a_l を q^l の係数にもつ重さ２，レベル Ｎのヘッケ作用素の同時固有関数 $\sum a_n q^n$ が存在する。

各自然数 N に対しレベルN の有限次元複素線形空間 $\mathrm{S}(\mathrm{N})_{\boldsymbol{c}}$ を定義し、これを保型形式の空間と呼ぶ。
これは形式べき級数$\left(\text{無限多項式 } \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots\right)$全体のなす空間の部分空間である。
この空間においては、ヘッケ作用素 (T_n)と呼ばれる自己準同型写像
$\mathrm{T}_n : \mathrm{S}(\mathrm{N})_{\boldsymbol{c}} \to \mathrm{S}(\mathrm{N})_{\boldsymbol{c}}$ が各自然数 $n \geq 1$ に対して定義されている。
保型形式は、

$$f(z) = f(z+1), \qquad \cdots\cdots\cdots\cdots\cdots\cdots ⑨$$
$$f(-1/z) = z^k f(z) \qquad \cdots\cdots\cdots\cdots\cdots\cdots ⑩$$

という等式を満たし、$z \to i\infty$ で正則であるような複素関数で、その名のとおり $z \to \frac{az+b}{cz+d}$ という変換に対し、形を保ち対称性のある関数である。これを $SL(2, \boldsymbol{Z})$ の保型形式ともいう。$SL(2, \boldsymbol{Z})$ は特殊線形群といい、成分が整数の２次正方行列で、式で表せば次のようになる。

$$SL(2, \boldsymbol{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \boldsymbol{Z}, ad - bc = 1 \right\} \qquad \cdots\cdots\cdots\cdots\cdots\cdots ⑪$$

保型形式の中でも特に重要なのが、正規化された同時固有カスプ形式と呼ばれるものである。
正規化された同時固有カスプ形式は、**ヘッケ作用素**（※11）を使って、

$$\boldsymbol{f} = \sum_{\boldsymbol{n=1}}^{\infty} a_{\boldsymbol{n}}(f)\, q^n \in \mathrm{S}\left(\mathrm{N}\right)_{\boldsymbol{c}} \qquad \cdots\cdots\cdots\cdots\cdots\cdots ⑫$$

（レベルNの保型形式）と定義される。

正規化された同時固有カスプ形式では、式⑫において、$\boldsymbol{f \neq 0}$ かつすべての自然数 $\boldsymbol{n \geq 1}$ に対して $\mathrm{T}_{\boldsymbol{n}}(f) = a_{\boldsymbol{n}}(f)f$ が成り立つ。

重さ２【保型形式の重さは⑩式の k を指す】，レベルＮのヘッケ作用素の同時固有関数であるカスプ形式 $\boldsymbol{f} = \sum_{\boldsymbol{n=1}}^{\infty} a_{\boldsymbol{n}}(f)\, q^n$ に対して、$\boldsymbol{K} = \boldsymbol{Q_p}$ ($\{a_n; n \geq 2\}$)とおくと $\boldsymbol{K/Q_p}$は有限次拡大であり、

連続的な規約表現 $\boldsymbol{\rho}_f$: $\boldsymbol{G_Q} = Gal(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \rightarrow GL_2(\boldsymbol{K})$ で、$Tr(\boldsymbol{\rho}_f(Frob_l)) = a_l$，$det(\boldsymbol{\rho}_f(Frob_l)) = l$ を満たすものが存在することが、アイヒラーと志村により示されている。

この表現は、複素数体上では複素トーラスのテイト加群をヘッケ作用素によって分解したときの $\boldsymbol{f}$ 成分への $\boldsymbol{G_Q}$ の作用から得られ、$\boldsymbol{f}$ 成分は楕円曲線となり、

$Tr\left(\boldsymbol{\rho}_f(Frob_l)\right) = Tr\left(\boldsymbol{\rho}_E(Frob_l)\right) = a_l$ となる。このようにして得られる楕円曲線をモジュラー楕円曲線という。

以上のことから、楕円曲線がモジュラーであることをいうためには、ある一つの素数 p に対して、

$\boldsymbol{\rho_p}$（テイト加群 $\mathrm{T}_{\boldsymbol{p}}(\mathrm{E})$ から導かれる表現）が保型形式からもたらされることを示せばよい。

これを示すために、ワイルズは素数 $p = 3$ を用いた。その理由は $\boldsymbol{\rho}_{E[3]}$ が規約のとき、$\boldsymbol{\rho}_{E[3]}$ はモジュラーであることがラングランズとタンネルによって証明されており、その前提が使えるためである。

$\boldsymbol{F}$ を標数 p の有限体、$\boldsymbol{\rho_0} : \boldsymbol{G_Q} \rightarrow GL_2(\boldsymbol{F})$ をモジュラーな表現とし、さらに次の（１）（２）（３）を満たすものとする。

（標数 p の体上の群の表現をモジュラー表現という。従って $\boldsymbol{\rho_0} : \boldsymbol{G_Q} \rightarrow GL_2(\boldsymbol{F})$ において、$\boldsymbol{F}$ は有限体 $\boldsymbol{Fp}$、GL_2 は２次の一般線形群だから、$\boldsymbol{\rho_0} : \boldsymbol{G_Q} \rightarrow GL_2(\boldsymbol{F})$ は、有限体 $\boldsymbol{Fp}$ 上の２次一般線形群への絶対ガロア群の表現 $\boldsymbol{\rho_0}$ を表す。それはモジュラー表現であることを示している）

（１）$\boldsymbol{\rho_0}$ は $\boldsymbol{Q}\left(\sqrt{(-1)^{\left(\frac{p-1}{2}\right)}p}\right)$ へ制限するとき、絶対既約である。

（絶対ガロア群 $G_Q = Gal(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$に対し、$\boldsymbol{Q}$ をその拡大体 $\boldsymbol{Q}\left(\sqrt{(-1)^{\left(\frac{p-1}{2}\right)}p}\right)$ に制限する、すなわち

$(-1)^{\left(\frac{p-1}{2}\right)}p$ において、$p \equiv 1(mod4)$ のとき(＋)、$p \equiv 3(mod4)$ のとき(－)となる。

従って、$p \equiv 1(mod4)$ では 5，13，17，29，37，41‥‥となり、このとき$\sqrt{\ }$ 内が(＋)となるので $\boldsymbol{Q}(\sqrt{5})$，$\boldsymbol{Q}(\sqrt{13})$，$\boldsymbol{Q}(\sqrt{17})$，$\boldsymbol{Q}(\sqrt{29})$，$\boldsymbol{Q}(\sqrt{37})$，$\boldsymbol{Q}(\sqrt{41})$‥‥、

$p \equiv 3(mod4)$ では 3，7，11，19，23，31‥‥となり、このとき$\sqrt{\ }$ 内が(－)となるので $\boldsymbol{Q}(\sqrt{-3})$，$\boldsymbol{Q}(\sqrt{-7})$，$\boldsymbol{Q}(\sqrt{-11})$，$\boldsymbol{Q}(\sqrt{-19})$，$\boldsymbol{Q}(\sqrt{-23})$，$\boldsymbol{Q}(\sqrt{-31})$‥‥である。

絶対既約とは、体を拡大しその拡大体が代数的閉包となっても、表現 $\boldsymbol{\rho}$ が規約であれば、$\boldsymbol{\rho}$ は絶対既約であるという。

（２）$det(\boldsymbol{\rho_0}) = \omega$　（ω =タイヒミュラー指標）

$det(\boldsymbol{\rho_0})$ は $\boldsymbol{\rho_0}$ の行列式の値（計算値）を表す。

タイヒミュラー指標 ω は、その定義から $\omega = \boldsymbol{Z}_p^{\times}$ であり、$\boldsymbol{Z}_p^{\times}$ は $\boldsymbol{Z}_p$ の 0 以外の元全体のなす乗法群を表す。$\boldsymbol{Z}_p$ は位数 p の巡回群 $\boldsymbol{Z/pZ}$ で、この行列式の値が $\boldsymbol{Z}_p^{\times}$ に一致するということを言っている。

（３）$\boldsymbol{\rho_0}$ を分解群に制限したときの条件をみたす。（Ｅが準安定な楕円曲線のとき、$\boldsymbol{\rho}_{E[p]}$ はこの条件を満たしている）

$\boldsymbol{O}$ を局所体の整数環、πを極大イデアルの生成元とし、

$\boldsymbol{\rho}：\boldsymbol{G_Q} \to GL_2(\boldsymbol{O})$を、$\boldsymbol{\rho}\ mod\ \pi = \boldsymbol{\rho_0}$ という表現とする。さらに $\boldsymbol{\rho}$ は次の３つの条件を満たすとする。

（ⅰ）$\boldsymbol{K_p}$ を $\boldsymbol{\rho}$ の核に対応する体とするとき、$\boldsymbol{K_p/Q}$ で分岐する素数は有限個

（ⅱ）$det(\boldsymbol{\rho_0}) = \kappa$　　（κ：円分指標）

（ⅲ）$\boldsymbol{\rho}$ を分解群に制限したときの条件（Ｅが準安定な楕円曲線のとき、$Tate$ 加群からできる表現はこの条件を満たしている）

以上の条件をみたすとき、$\boldsymbol{\rho}$ は保型形式からもたらされるということがいえる。

$\boldsymbol{G_Q} \to GL_2(\boldsymbol{F_3})$ という既約表現はモジュラーであることが証明されているので、楕円曲線がモジュラーであることを証明するために、$GL_2(\boldsymbol{F_3})$ が可解群であることを利用する。

３等分点からできる表現 $\boldsymbol{\rho}_{E[3]}$を$\boldsymbol{Q}(\sqrt{-3})$ の絶対ガロア群 $Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q}\sqrt{-3})$ に制限しても絶対既約とすると、Ｅはモジュラーな楕円曲線である。

ワイルズは５等分点を補助的に巧妙に使うことによって、既約性の条件も除けることを示し、最終的にすべての準安定な楕円曲線がモジュラーであることを証明した。

有理数体 $\boldsymbol{Q}$ 上の巨大な群である絶対ガロア群 $\boldsymbol{G_Q}$ が、数論的対象（例えば楕円曲線や保型形式）に作用することにより、その姿の一端を現す。楕円曲線上の有限個の点からなる集合 $\boldsymbol{V}$ がこの操作により閉じているとき、$\boldsymbol{V}$ には絶対ガロア群 $\boldsymbol{G_Q}$ が作用し、$\boldsymbol{V}$ はガロア表現の一つの例になる。

一つの楕円曲線に対してこの様な集合は無数にあり、そのどれもがガロア表現になっている。その中でも特に重要なのが、各素数 p と自然数 n ごとに p^{2n} 個の元から成るガロア表現 $\boldsymbol{V}(\mathrm{E},\ p^n)$ である。

一方、特別な保型形式 $f(z)$ からも、作り方はもう少し抽象的になるが、同様なガロア表現 $\boldsymbol{V}(f,\ p^n)$ を作ることができる。

このようにして、楕円曲線と保型形式の双方から、それぞれ一つずつガロア表現の系列 $\boldsymbol{V}(\mathrm{E},\ p^n)$, 及び、$\boldsymbol{V}(f,\ p^n)$ $(n = 1,\ 2,\ 3, 、、、、、)$ が得られる。それぞれのガロア表現を対応させるために、Ｅとf を対応させる必要があるが、そのためにはＥに対して$\boldsymbol{V}(\mathrm{E},\ p^n)$ と同じ性質を持つ$\boldsymbol{V}(f,\ p^n)$ を生ずる $f(z)$ を探さなくてはならない。これは非常に難しいことであるが、$\boldsymbol{V}(\mathrm{E},\ 2^1)$と$\boldsymbol{V}(\mathrm{E},\ 3^1)$ についてだけは例外的に、ラングランズとタンネルによってそのような $f(z)$ の存在が証明されている。

そこで$\boldsymbol{V}(\mathrm{E},\ p^1)$と$\boldsymbol{V}(f,\ p^1)$ とが同じ性質を持つと仮定したとき、$\boldsymbol{V}(\mathrm{E},\ p^2)$と$\boldsymbol{V}(g,\ p^2)$ とが同じ性質を持つような $g(z)$ が見つけられないかを考える。これは一般に、$\boldsymbol{V}(\mathrm{E},\ p^n)$と$\boldsymbol{V}(f,\ p^n)$ とが同じ性質を持つと仮定したとき、$\boldsymbol{V}(\mathrm{E},\ p^{n+1})$と$\boldsymbol{V}(g,\ p^{n+1})$ とが同じ性質を持つような $g(z)$ が見つけられないかという問題である。この問題を解決するために、メイザーによる「ガロア表現の変形理論」【モジュライ[楕円曲線は、全体としてどのくらい種類があるかを代数幾何学的に捉えるための手法]の局所理論の考え方の枠組みをガロア表現に適用したもの。体上の楕円曲線はモジュライ空間の点を与えるが、モジュライ空間全体ではなく、その点の周りでのモジュライ空間の局所的な様子だけを詳しく調べる】を用いる。

この理論によれば、$\boldsymbol{V}(\mathrm{E},\ p^1)$ のある種の変形の全体を仕切る環 $\boldsymbol{R}$【ガロア表現の普遍変形環：ガロア表現の変形理論における形式的モジュライ空間の座標環のこと】と $\boldsymbol{V}(f,\ p^1)$ のある種の変形の全体を仕

切る環 $\boldsymbol{T}$ とがあって、 $\boldsymbol{R}=\boldsymbol{T}$ を示せばよい。
「$\boldsymbol{R}=\boldsymbol{T}$」はワイルズが谷山－志村予想を部分的に証明することでフェルマー予想証明のためにあみだしたテクニックと考えることができる。

$\boldsymbol{\rho_0}$ は前記（1）～（3）の通りとする。このとき、(ⅰ）～（ⅲ）を満たす $\boldsymbol{\rho}$ に対し次のような性質を満たす環 $\boldsymbol{R}$ とガロア表現、$\boldsymbol{\rho_R}:\boldsymbol{G_Q}\to GL_2(\boldsymbol{R})$ が存在している。

条件（ⅰ）～（ⅲ）を満たす $\boldsymbol{\rho}$ があると、$\boldsymbol{R}\to\boldsymbol{O}$ という環準同型が存在して、この環準同型写像からできる準同型写像 $GL_2(\boldsymbol{R})\to GL_2(\boldsymbol{O})$ と $\boldsymbol{\rho_R}$ との合成、$\boldsymbol{G_Q}\to GL_2(\boldsymbol{R})\to GL_2(\boldsymbol{O})$ が $\boldsymbol{\rho}$ と同値である。

一方、条件（ⅰ）～（ⅲ）に、条件「$\boldsymbol{\rho}$ は保型形式からくる」を加えても、普遍的な環 $\boldsymbol{T}$ とガロア表現、$\boldsymbol{\rho_T}:\boldsymbol{G_Q}\to GL_2(\boldsymbol{T})$ が存在して、このような条件をみたすモジュラーな $\boldsymbol{\rho}$ はすべて $\boldsymbol{\rho_T}$ から得られる。

すなわち、そのような $\boldsymbol{\rho}$ があるとすると、$\boldsymbol{T}\to\boldsymbol{O}$ という環準同型が存在して、この準同型写像からできる準同型写像 $GL_2(\boldsymbol{T})\to GL_2(\boldsymbol{O})$ と $\boldsymbol{\rho_T}$ の合成、$\boldsymbol{G_Q}\xrightarrow{\rho_T} GL_2(\boldsymbol{T})\to GL_2(\boldsymbol{O})$ が $\boldsymbol{\rho}$ と同値になるのである。
$\boldsymbol{T}$ はヘッケ環【ヘッケ作用素からできる環】から作られる。このような変形理論を使うと、「$\boldsymbol{\rho}$ は保型形式からくる」ということが単に「$\boldsymbol{R}=\boldsymbol{T}$」と表せる。

$\boldsymbol{R}$ と $\boldsymbol{T}$ の定義から、$\boldsymbol{R}\to\boldsymbol{T}$ という環準同型があって、全射であることが示せる。よって、この写像が同型写像であることを示せばよいことになる。

以下「岩波講座 現代数学の展開 Fermat 予想１」を引用する。

$\boldsymbol{R}=\{\boldsymbol{\rho}:\boldsymbol{G_Q}\to GL_2(\boldsymbol{O})\mid \boldsymbol{\rho}$ は$\bar{\boldsymbol{\rho}}$ の $\boldsymbol{O}$ への準安定な持ち上げで、その行列式$det\,\boldsymbol{\rho}$ は円分指標である$\}$

$\boldsymbol{T}=\{\boldsymbol{K}$ 係数の素形式［正規化された同時固有新カスプ形式］$\boldsymbol{f}\mid$ 有限個をわたる素数 p に対し$a_p(\boldsymbol{f})\equiv Tr\,\bar{\boldsymbol{\rho}}(\varphi_p)\}$
とする。

$\boldsymbol{f}$ に対し、$\boldsymbol{f}$ に伴う l 進表現 $\boldsymbol{\rho_f}$ を対応させることにより、単射 $\varphi:\boldsymbol{T}\to\boldsymbol{R}$ が定義される。
定理の主張はこの写像が全単射ということである。このままでは、$\boldsymbol{T}$ も $\boldsymbol{R}$ も無限集合なので扱いにくい。そこで次のようにそれぞれの部分集合を考える。

$\sum$ を素数の有限集合とし、

$\boldsymbol{R_\Sigma}=\{\boldsymbol{\rho}\in\boldsymbol{R}\mid \boldsymbol{\rho}$ の分岐は$\sum$ 以外の素数では$\bar{\boldsymbol{\rho}}$ の分岐と同じ程度である$\}$

$\boldsymbol{T_\Sigma}=\{\boldsymbol{f}\in\boldsymbol{T}\mid \boldsymbol{\rho_f}$ の分岐は$\sum$以外の素数では$\bar{\boldsymbol{\rho}}$ の分岐と同じ程度である$\}$ とおく。

これらに対しても同様に単射 $\boldsymbol{\varphi_\Sigma}:\boldsymbol{T_\Sigma}\to\boldsymbol{R_\Sigma}$ が定義される。
$\boldsymbol{R}=\bigcup_{\boldsymbol{\Sigma}}\boldsymbol{R_\Sigma}$ だから、$\sum$ ごとに $\boldsymbol{\varphi_\Sigma}$ が全単射であることを示せば、φ が全単射であることが示せる。
写像 $\boldsymbol{\varphi_\Sigma}:\boldsymbol{T_\Sigma}\to\boldsymbol{R_\Sigma}$ が全単射であることを示すための重要な一歩は、これを可換環論で解釈することである。$\boldsymbol{O}$ 上の環 $\boldsymbol{R_\Sigma}$，$\boldsymbol{T_\Sigma}$ と $\boldsymbol{O}$ 上の環の準同型 $\boldsymbol{f_\Sigma}:\boldsymbol{R_\Sigma}\to\boldsymbol{T_\Sigma}$ で次の、a，b，c の性質を持つものを定義する。

a　$\boldsymbol{R_\Sigma}=\{\boldsymbol{O}$ 上の環の準同型 $\boldsymbol{R_\Sigma}\to\boldsymbol{O}\}$

b　$\boldsymbol{T_\Sigma}=\{\boldsymbol{O}$ 上の環の準同型 $\boldsymbol{T_\Sigma}\to\boldsymbol{O}\}$

c　写像 $\boldsymbol{\varphi_\Sigma}:\boldsymbol{T_\Sigma}\to\boldsymbol{R_\Sigma}$ は、写像$\{\boldsymbol{O}$ 上の環の準同型 $\boldsymbol{T_\Sigma}\to\boldsymbol{O}\}\longrightarrow\{\boldsymbol{O}$ 上の環の準同型 $\boldsymbol{R_\Sigma}\to\boldsymbol{O}\}$と等しい。

$$\ni g \qquad \mapsto \qquad \ni g\circ\boldsymbol{f_\Sigma}$$

写像 $\boldsymbol{\varphi_\Sigma}:\boldsymbol{T_\Sigma}\to\boldsymbol{R_\Sigma}$ が全単射であることを示すことは、環の準同型 $\boldsymbol{f_\Sigma}:\boldsymbol{R_\Sigma}\to\boldsymbol{T_\Sigma}$ が同型であることを示すことに帰着される。
ここで、環 $\boldsymbol{R_\Sigma}$ が満たすべき性質を書き直すと次のようになる。

$$\{\boldsymbol{O}\text{ 上の環の準同型}\boldsymbol{R_\Sigma}\to\boldsymbol{O}\}=\left\{\boldsymbol{\rho}\;\middle|\;\begin{array}{l}\boldsymbol{\rho}\text{ は}\bar{\rho}\text{ の}\boldsymbol{O}\text{ への持ち上げで、}\ det\,\boldsymbol{\rho}\text{ は円分指標であり、}\\ \boldsymbol{\rho}\text{ の分岐は}\sum\text{ 以外の素数では}\bar{\rho}\text{ の分岐と同じ程度である}\end{array}\right\}$$

この性質を、$\boldsymbol{O}$ への準同型だけでなく、$\boldsymbol{O}$ 上の任意の環への準同型について課すことによって環 $\boldsymbol{R_\Sigma}$ を定義する。$\boldsymbol{O}$上の任意の環 $\boldsymbol{A}$ について、

$$\{\boldsymbol{O}\text{ 上の環の準同型}\boldsymbol{R_\Sigma}\to\boldsymbol{A}\}=\left\{\boldsymbol{\rho}\;\middle|\;\begin{array}{l}\boldsymbol{\rho}\text{ は}\bar{\rho}\text{ の}\boldsymbol{A}\text{ への持ち上げで、}\ det\,\boldsymbol{\rho}\text{ は円分指標であり、}\\ \boldsymbol{\rho}\text{ の分岐は}\sum\text{ 以外の素数では}\bar{\rho}\text{ の分岐と同じ程度である}\end{array}\right\}$$

がなりたつ、という性質によって環 $\boldsymbol{R_\Sigma}$ がただ１つだけ定まるのである。

代数幾何の変形理論との類似により、この環 $\boldsymbol{R_\Sigma}$ のことを変形環という。

環 $\boldsymbol{T_\Sigma}$ はヘッケ環の部分環として定義される。$\bar{\boldsymbol{\rho}}$ の導手 $\boldsymbol{N_{\bar\rho}}$ の倍数 $\boldsymbol{N_\Sigma}$ をうまく定めて、

$\boldsymbol{T_\Sigma}=\{\boldsymbol{f}\in\boldsymbol{T}\,|\,f\text{ のレベルは }\boldsymbol{N_\Sigma}\text{ の約数}\}$ となるようにとる。

$\boldsymbol{\Phi(N_\Sigma)_{K,\bar\rho}}$ を $\boldsymbol{K}$ 上のレベルが $\boldsymbol{N_\Sigma}$ の約数の素形式 $\boldsymbol{f}$ で、有限個をわたる素数 p に対し $a_p(\boldsymbol{f})\equiv Tr\,\bar{\boldsymbol{\rho}}(\varphi_p)$ をみたすものからなる有限集合とする。

それぞれの素形式 $\boldsymbol{f}=\sum_{\boldsymbol{n=1}}^{\infty}a_{\boldsymbol{n}}(f)\,q^n\in\boldsymbol{\Phi(N_\Sigma)_{K,\bar\rho}}$ に対し、

$\boldsymbol{K_f}$ を $\boldsymbol{K}$ 上 $a_{\boldsymbol{n}}(f)$，$n\in\boldsymbol{N}$ で生成される体とし、$\boldsymbol{O_f}$ をその整数環とする。$\boldsymbol{O}$ 上の環準同型 $\boldsymbol{R}\to\boldsymbol{O_f}$ を定める。

$\boldsymbol{f}$ に伴う l 進表現 $\boldsymbol{\rho_f}:\boldsymbol{G_Q}\to GL_2(\boldsymbol{O_f})$ は、$\bar{\boldsymbol{\rho}}$ の $\boldsymbol{O_f}$ への持ち上げで、$det\,\boldsymbol{\rho_f}$ は円分指標であり、

$\boldsymbol{\rho_f}$ の分岐は $\sum$ 以外の素数では $\bar{\boldsymbol{\rho}}$ の分岐と同じ程度である。

したがって $\boldsymbol{R_\Sigma}$ の定義により、環の準同型 $\psi_{\boldsymbol{f}}:\boldsymbol{R_\Sigma}\to\boldsymbol{O_f}$ が定まる。

これの積 $\boldsymbol{\Psi_\Sigma}:\boldsymbol{R_\Sigma}\to\prod_{f\in\Phi(N_\Sigma)_{K,\bar\rho}}\boldsymbol{O_f}$ の像が $\boldsymbol{T_\Sigma}$ である。環 $\boldsymbol{T_\Sigma}$ は被約ヘッケ環、または単にヘッケ環と呼ぶ。

環の準同型 $\boldsymbol{f_\Sigma}:\boldsymbol{R_\Sigma}\to\boldsymbol{T_\Sigma}$ は、$\boldsymbol{\Psi_\Sigma}:\boldsymbol{R_\Sigma}\to\prod_{f\in\Phi(N_\Sigma)_{K,\bar\rho}}\boldsymbol{O_f}$ によって引き起こされる全射準同型とする。

これが、$\boldsymbol{R_\Sigma}$，$\boldsymbol{T_\Sigma}$，$\boldsymbol{f_\Sigma}$ の定義の方法である。以上の定義をもとに、

l を３以上の素数とし、$\boldsymbol{O}$ を $\boldsymbol{Q_l}$ の有限次拡大 $\boldsymbol{K}$ の整数環とする。$\boldsymbol{F}$ を $\boldsymbol{O}$ の剰余体とし、$\bar\rho:\boldsymbol{G_Q}\to GL_2(\boldsymbol{F})$ を準安定な、規約で保型的な法 l 表現で、$det\ \bar\rho:\boldsymbol{G_Q}\to\boldsymbol{F}^\times$ が円分指標であるものとする。素数の有限集合 $S_{\bar\rho}$ を $S_{\bar\rho}=\{p\text{ は素数}|\bar\rho\text{は}p\text{でよくない}\}$ と定める。

$\sum$ を素数の有限集合で、$\sum\cap S_{\bar\rho}=\phi$、$l\in\sum$ ならば $\bar\rho$ は l でよく、かつ通常という条件を満たすとき、標準全射 $\boldsymbol{f_\Sigma}:\boldsymbol{R_\Sigma}\to\boldsymbol{T_\Sigma}$ は同型であることが証明される。

$\bar\rho$ の $\boldsymbol{O}$ への準安定なもちあげ $\rho:\boldsymbol{G_Q}\to GL_2(\boldsymbol{O})$ は、その行列式 $det\ \rho:\boldsymbol{G_Q}\to\boldsymbol{O}^\times$ が円分指標ならば、

$\sum=\sum(\rho)=\{p\,|\,\bar\rho\text{は}p\text{でよいが}\rho\text{は}p\text{でよくない}\}$ とすると、$\boldsymbol{f_\Sigma}:\boldsymbol{R_\Sigma}\to\boldsymbol{T_\Sigma}$ は同型だから、ρ はレベルN_Σ で保型的であり、ρ の導手は $\boldsymbol{f}$ のレベル N に等しいので、ρ はレベルN_ρ で保型的である。

すなわち、$\boldsymbol{K}$ 係数でレベルがN_ρ の約数の素形式 $\boldsymbol{f}$ で、すべての素数 $p\nmid N_\rho l$ に対し、

$det(1-\rho(\varphi_p)t)=1-a_p(f)t+pt^2$ となるものが存在することが証明された。

（※１）「すべての楕円曲線はモジュラーである」について

楕円曲線は複素平面において、「【図２】複素トーラスと楕円曲線のつながり」に示すように、２組の複素数$(\omega_1,\ \omega_2)$で作られる格子からできるトーラスというドーナツ型の立体図形で表される。

楕円曲線の全体集合は格子の全体集合と同じものとみなせる。この格子はワイエルストラスの$\wp$関数（ペー関数）呼ばれる関数を使って、楕円曲線上の点と一対一の対応がつくことが示されている。

詳しくは（※８「**複素数体上の楕円曲線**」参照）

$\wp$関数は、複素平面内の格子$\mathrm{L} = \mathrm{Z}\omega_1 + \mathrm{Z}\omega_2$を決めるごとに決まる複素変数関数$\wp(\mathrm{z})$で次の式で定義される。

$$\wp(z) = \frac{1}{z^2} + \sum_{w \epsilon L \neq \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

この関数はLの任意の元 $w \epsilon \mathrm{L}$ に対し、定数 Z が変化すると、正則関数の等角性（複素数を受け取って複素数の値を返す関数で、その関数がすべての点で微分可能な関数であれば、その関数による写像は等角写像である）から異なったトーラスが現れる。このことから楕円曲線は複素解析的に見て同一視できないものが無数に存在する。これが楕円曲線のモジュライである。

楕円曲線の全体からなる集合を格子の相似で分類し、その各分類に無数に存在するトーラスの中から１つずつ代表を選んだときにできる集合を、楕円曲線のモジュライ空間と呼んでいる。すなわち、楕円曲線は格子を適当に相似変換すればモジュラー群の基本領域、すなわちモジュライ空間の点とみなすことができる。従って楕円曲線の全体集合とは、格子の全体集合と同じものとみなせる。

複素平面の上側半分を複素上半平面Hと呼び、そこに作用する基本群として整数を成分とする行列

$SL(2,\boldsymbol{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\ ad - bc = 1,\ a,b,c,d \in \boldsymbol{Z} \right\}$ を考える。

これをモジュラー群といい、H上に１次分数変換として作用する。

この作用は、$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \dfrac{az+b}{cz+d}$ と定義される。

モジュラー群の基本領域上の関数であり、かつモジュラー群の作用で他の基本領域に移して考えたときの関数値がある条件に従う関数を保型形式という。

その条件とはモジューラー群$SL(2,\boldsymbol{Z})$の任意の元γに対し、

$f(\gamma \cdot z) = (cz + d)^k f(z)\ (z \in H)$を満たすことである。このような条件を満たす上半平面H上で定義される関数$f(z)$を重さkの保型形式と呼ぶ。

（※２）「有理数体 Q 上の楕円曲線Ｅ」について

楕円曲線は、３次曲線にいくつか条件を付けたものをいう。

$\boldsymbol{K}$を代数体【$\boldsymbol{Q}$の有限次拡大体】あるいは有限体【整数を素数pで割った余りの数による集合】とする。

３次曲線の一般形は次のように表され、これを$\boldsymbol{K}$上の３次曲線と呼ぶ。

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\ (a_i \in \boldsymbol{K})$$

$\boldsymbol{K}$の標数【体の特徴を表すもので、ある体の元m（正の整数）をその体の任意の元aに対して$ma = 0$が成り立つmのうち最小のものを体の標数という。０に１をいくつ足したら０になるかといえば分かりやすい。有理数体($\boldsymbol{Q}$)，実数体($\boldsymbol{R}$)，複素数体 ($\boldsymbol{C}$) の標数は０、有限体では１をp回足せば０になるので、

$(\boldsymbol{Z_p})$ の標数は p である】が２でなければ、変数変換 $y=\frac{y-a_1x-a_3}{2}$ によって、

$y^2=4x^3+b_2x^2+2b_4x+b_6$ $(y^2=ax^3+bx^2+cx+d)$ の形になる。

さらに、$\boldsymbol{K}$ の標数が、２でも３でもなければ、変数変換 $x=\frac{x-3b_2}{2}$，$y=\frac{y}{108}$ によって、

$y^2=x^3-27c_4x-54c_6$ $(y^2=x^3+bx+c)$ の形になる。

ここで、$b_2=a_1^2+4a_2$，$b_4=2a_4+a_1a_3$，$b_6=a_3^2+4a_6$，$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$

$c_4=b_2^2-24b_4$，$c_6=-b_2^3+36b_2b_4-216b_6$ である。

$\Delta(\mathrm{E})=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6$ を楕円曲線Ｅの判別式という。

この判別式を用いて楕円曲線を次のように定義する。

$\Delta(\mathrm{E})\neq 0$ のとき、Ｅは $\boldsymbol{K}$ 上の楕円曲線という。$\boldsymbol{K}=\boldsymbol{Q}$ のとき、$\Delta(\mathrm{E})\neq 0$ であれば楕円曲線のグラフに特異点がなく、$\Delta(\mathrm{E})=0$ であれば特異点を持つ。特異点は２種類あり、１つは尖った部分を持つカスプ型（$c_4=0$），もう１つは自己交叉する点を持つノード型（$c_4\neq 0$）である。

$\boldsymbol{K}=\boldsymbol{Q}$（標数０）であれば、必ず $y^2=x^3+ax+b$ $(a,b\in\boldsymbol{Q})$ の形に変形できる。

楕円曲線Ｅの係数が全て整数のとき、$\boldsymbol{Q}$ 上の楕円曲線という。この係数を $mod\ p$ して考える、つまり有限体 $\boldsymbol{F_p}$ 上で考えることをＥの p における還元という。

E_p は常に楕円曲線〔$\Delta(\mathrm{E}_p)\neq 0$〕になるとは限らず、$p$ が判別式 $\Delta(\mathrm{E})$ を割り切るような素数の時は $\Delta(\mathrm{E}_p)=0$ となり楕円曲線にはならない。そこで、還元しても楕円曲線である場合、Ｅは p で『よい還元を持つ』という。逆に、$\Delta(\mathrm{E}_p)=0$ のときは特異点が現れ、$\boldsymbol{F_p}$ 上の楕円曲線でなくなり、『悪い還元を持つ』という。特異点がノード型の場合を乗法的（半安定）還元、カスプ型の場合を加法的（不安定）還元を持つという。

（※３）「正規化された同時固有カスプ形式」について

正規化された同時固有カスプ形式とは、保型形式の中で特別なものである。

保型形式 $f(z)$ は複素上半平面 $\mathrm{H}=\{z\in\boldsymbol{C}\mid I_m(z)>0\}$ の有理型正則関数で、その中で複雑な変数変換

$z\to\frac{az+b}{cz+d}$ $(a,b,c,d\in\boldsymbol{Z}$ で $ad-bc=1$ を満たす$)$ に対して不変性を持つ特殊な性質の関数である。

$a=b=d=1$，$c=0$ とすると、$ad-bc=1$ を満たすので、$z\to\frac{1z+1}{0z+1}=z+1$ という変換に対して不変であり $f(z)=f(z+1)$ となるから、周期１の周期関数である。すべての周期関数はフーリエ級数に展開でき、式で表すと $f(z)=\sum_{n=-\infty}^{\infty}a_n e^{2\pi inz}$ となる。

ここで $e^{2\pi iz}=q$ と変数変換すれば、$f(z)$ は原点の周りで正則関数なのでローラン展開して、

$f(z)=\sum_{n=-\infty}^{\infty}a_n q^n$ となる。

正規化された同時固有カスプ形式は、保型形式の中で負のベキ乗の項が０、すなわち

$n<0$ のとき $a_n=0$ となるもの（モジュラー形式という）で、さらに $a_0=0$ を満たすものであり、正規化された同時固有カスプ形式は、$n=-\infty\to n=1$ として、

$f(z)=\sum_{n=1}^{\infty} a_n q^n$　と書かれる。ここで、$a_n(n \geqq 1)$ は有理数である。

（※４）「楕円曲線Ｅのｎ等分点」について

有限体 $\boldsymbol{F_p}$ 上の楕円曲線において、具体的に $y^2=x^3+x$ の５等分点を計算してみる。

等分点は有理多項式で表され、等分多項式の公式が示されている。

$y^2=x^3+ax+b$ の等分点は、$\mathrm{P}(x,y) \in \boldsymbol{F_5} \times \boldsymbol{F_5}$ という群構造で５×５＝２５個の元を持つ。

等分多項式 $\psi_m(x,y)$ は以下のとおりである。

$\psi_0(x,y)=0$

$\psi_1(x,y)=1$

$\psi_2(x,y)=2y$

$\psi_3(x,y)=3x^4+6ax^2+12bx-a^2$

$\psi_4(x,y)=4y(x^6+5ax^4+20bx^3-5a^2x^2-8b^2-a^3)$

$m=5$ からは非常に複雑な式となり、

$$\psi_5(x,y)=-27x^{12}-162ax^{10}-324bx^9-297a^2x^8-1296abx^7+(32y^4-108a^3-1296b^2)x^6$$
$$-1080a^2bx^5+(160ay^4+99a^4-2592ab^2)x^4+(640by^4+432a^3b-1728b^3)x^3$$
$$+(-160a^2y^4-18a^5+432a^2b^2)x^2+(-128aby^4-36a^4b)x+(-32a^3-256b^2)y^4+a^6$$

$\psi_6(x,y)$ 以上は省略。

$\psi_m(x,y)$ は漸化式で示され、以下のとおりである。

$$\psi_{2m+1}=\psi_{m+2}\cdot{\psi^3}_m-\psi_{m-1}\cdot{\psi^3}_{m+1} \qquad (m \geq 2)$$

$$\psi_{2m}=\frac{\psi_m}{2y}\left(\psi_{m+2}\cdot{\psi^2}_{m-1}-\psi_{m-2}\cdot{\psi^2}_{m+1}\right) \quad (m \geq 3)$$

５等分点の多項式　$\psi_5(x,y)$ において、$y^2=x^3+x$ の場合は $a=1,\ b=0$ なので、

$$\psi_5(x,y)=-27x^{12}-162x^{10}-297x^8+(32y^4-108)x^6+(160y^4+99)x^4$$
$$+(-160y^4-18)x^2+(-32)y^4+1$$

$(y^2)^2=(x^3+x)^2$ を入れて $\psi_5(x,y)=0$ とすると、x についての１２次方程式となる。

$$\psi_5(x,y)=-27x^{12}-162x^{10}-297x^8+[32(x^3+x)^2-108]x^6+[160(x^3+x)^2+99]x^4$$
$$+[-160(x^3+x)^2-18]x^2+(-32)(x^3+x)^2+1=0$$

この方程式から１２の点が求められ、さらに $y^2=x^3+x$ は虚数乗法を持つ楕円曲線であり、$(x,y) \to (-x,iy)$ としても成り立つので、合計２４の点が得られ、無限遠点を加えて合計２５の点が求められる。上式 $\psi_5(x,y)$ を整理すると、

$$5x^{12}+62x^{10}-105x^8-300x^6-125x^4-50x^2+1=0$$

この式は２つの多項式の積に分解できて次のようになる。

$$(5x^4+2x^2+1)(x^8+12x^6-26x^4-52x^2+1)=0$$

これを解いて、第１の（　）$=0$ より、$P_1, 2P_1, 3P_1, 4P_1$ ４つの点が得られる。y 座標は、$\sqrt{x^3+x}$ で表すと、

$$P_1(x_{11},\ y_{11})=\left(\sqrt{\frac{-1+2i}{5}},\ \sqrt{{x_{11}}^3+x_{11}}\right),\quad 2P_1(x_{12},\ y_{12})=\left(-\sqrt{\frac{-1+2i}{5}},\ \sqrt{{x_{12}}^3+x_{12}}\right)$$

$$3P_1(x_{13},\ y_{13})=\left(\sqrt{\frac{-1-2i}{5}},\ \sqrt{{x_{13}}^3+x_{13}}\right),\quad 4P_1(x_{14},\ y_{14})=\left(-\sqrt{\frac{-1-2i}{5}},\ \sqrt{{x_{14}}^3+x_{14}}\right)$$

第２の（　　）＝０より、$P_2, 2P_2, 3P_2, 4P_2,\ P_3, 2P_3, 3P_3, 4P_3$ ８つの点が得られる。

$$P_2(x_{21},\ y_{21})=\left(\sqrt{-3+2\sqrt{5}+2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{21}}^3+x_{21}}\right)\quad 2P_2(x_{22},\ y_{22})=\left(-\sqrt{-3+2\sqrt{5}+2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{22}}^3+x_{22}}\right)$$

$$3P_2(x_{23},\ y_{23})=\left(\sqrt{-3+2\sqrt{5}-2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{23}}^3+x_{23}}\right)\quad 4P_2(x_{24},\ y_{24})=\left(-\sqrt{-3+2\sqrt{5}-2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{24}}^3+x_{24}}\right)$$

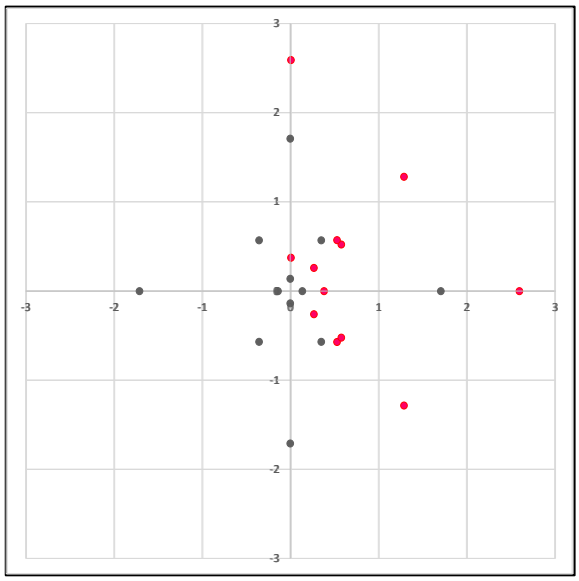
$$P_3(x_{31},\ y_{31})=\left(i\sqrt{-3+2\sqrt{5}+2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{31}}^3+x_{31}}\right)\ 2P_3(x_{32},\ y_{32})=\left(-i\sqrt{-3+2\sqrt{5}+2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{32}}^3+x_{32}}\right)$$

$$3P_3(x_{33},\ y_{33})=\left(i\sqrt{-3+2\sqrt{5}-2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{33}}^3+x_{23}}\right)4P_3(x_{34},\ y_{34})=\left(-i\sqrt{-3+2\sqrt{5}-2\sqrt{5-2\sqrt{5}}},\ \sqrt{{x_{34}}^3+x_{34}}\right)$$

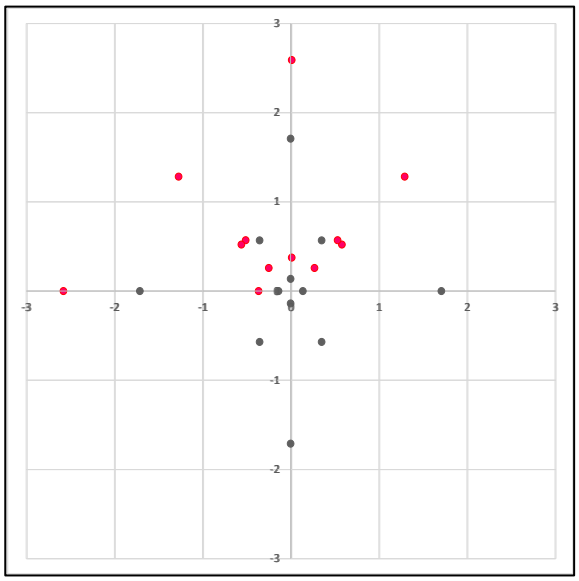
$x\to -x,\ \mathrm{y}\to iy$ とすれば、さらに１２の点が得られ、無限遠点を加えて合計２５の点が求められる。
求められた２４点を小数点下３桁で示すと**表１**のようになる。

表１　$y^2=x^3+x$ ５等分点

等分点	１２次方程式の解		等分点	虚数乗法より	
	x	y		$-x$	iy
$P_1(x_{11},\ y_{11})$	$0.352+0.569i$	$0.571+0.522i$	$P'_1(x'_{11},\ y'_{11})$	$-0.352-0.569i$	$-0.522+0.571i$
$2P_1(x_{12},\ y_{12})$	$-0.352-0.569i$	$0.522-0.571i$	$2P'_1(x'_{12},\ y'_{12})$	$0.352+0.569i$	$0.571+0.522i$
$3P_1(x_{13},\ y_{13})$	$0.352-0.569i$	$0.571-0.522i$	$3P'_1(x'_{13},\ y'_{13})$	$-0.352+0.569i$	$0.522+0.571i$
$4P_1(x_{14},\ y_{14})$	$-0.352+0.569i$	$0.522+0.571i$	$4P'_1(x'_{14},\ y'_{14})$	$0.352-0.569i$	$-0.571+0.522i$
$P_2(x_{21},\ y_{21})$	1.710	2.591	$P'_2(x'_{21},\ y'_{21})$	-1.710	$2.591i$
$2P_2(x_{22},\ y_{22})$	-1.710	$2.591i$	$2P'_2(x'_{22},\ y_{,22})$	1.710	-2.591
$3P_2(x_{23},\ y_{23})$	0.138	0.375	$3P'_2(x'_{23},\ y'_{23})$	-0.138	$0.375i$
$4P_2(x_{24},\ y_{24})$	-0.138	$0.375i$	$4P'_2(x'_{24},\ y'_{24})$	0.138	-0.375
$P_3(x_{31},\ y_{31})$	$1.710i$	$1.283-1.283i$	$P'_3(x'_{31},\ y'_{31})$	$-1.710i$	$1.283+1.283i$
$2P_3(x_{32},\ y_{32})$	$-1.710i$	$1.283+1.283i$	$2P'_3(x'_{32},\ y'_{32})$	$1.710i$	$-1.283+1.283i$
$3P_3(x_{33},\ y_{33})$	$0.138i$	$0.260+0.260i$	$3P'_3(x'_{33},\ y'_{33})$	$-0.138i$	$-0.260+0.260i$
$4P_3(x_{34},\ y_{34})$	$-0.138i$	$0.260-0.260i$	$4P'_3(x'_{34},\ y'_{34})$	$0.138i$	$0.260+0.260i$



図Ａ　等分点（方程式の解による）



図Ｂ　等分点（虚数乗法による）

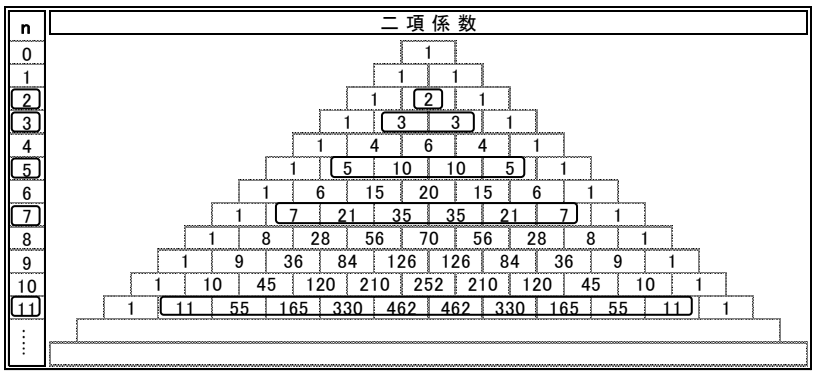
等分点の x,y 座標は、実数，純虚数，複素数のいずれかで与えらているので、すべての点を示すためには４次元の座標が必要となる。図Ａは「１２次方程式の解」、図Ｂは「虚数乗法」により求めた点について、x 座標を黒，y 座標を赤で２次元複素平面にプロットしたものである。

x 座標については $x \to -x$ から、縦軸に対する対称移動であり、結果的にＡ，Ｂとも同じ位置となっている。y 座標については $y \to iy$ から、反時計回りに９０° 回転した位置に移動している。従って、x,y の組み合わせとして表される点は全て異なったものである。

この等分点に対し絶対ガロア群の元が作用するが、その作用は行列で表わされる。

（※５）「幾何的フロベニウスと呼ばれる自己準同型」について

$(a+b)^n$ を二項展開すると各項の係数は次の**図Ｃ**のようになる。ここで n が素数 p のとき、図では２，３，５，７，１１のとき、両端の１以外の係数は全て p で割り切れるため、有限体 F_p で考えれば、$f(a+b)=(a+b)^p = a^p+b^p = f(a)+f(b)$ が成り立つので準同型写像である。



図Ｃ　二項係数

例えば、$F_5=\{0,1,2,3,4\}$ において $(3+4)^5$ を考えると $3+4=2$だから、$(3+4)^5 = 2^5 = 32 = 2$

一方、$3^5+4^5 = 243+1024 = 1267 = 2$となり、$(3+4)^5 = 3^5+4^5$ が成り立っていることがわかる。

（※６）「楕円曲線Ｅの元が群構造をなす」について

例として、楕円曲線 Ｅ：$y^2=x^3+3$ について考えてみる。

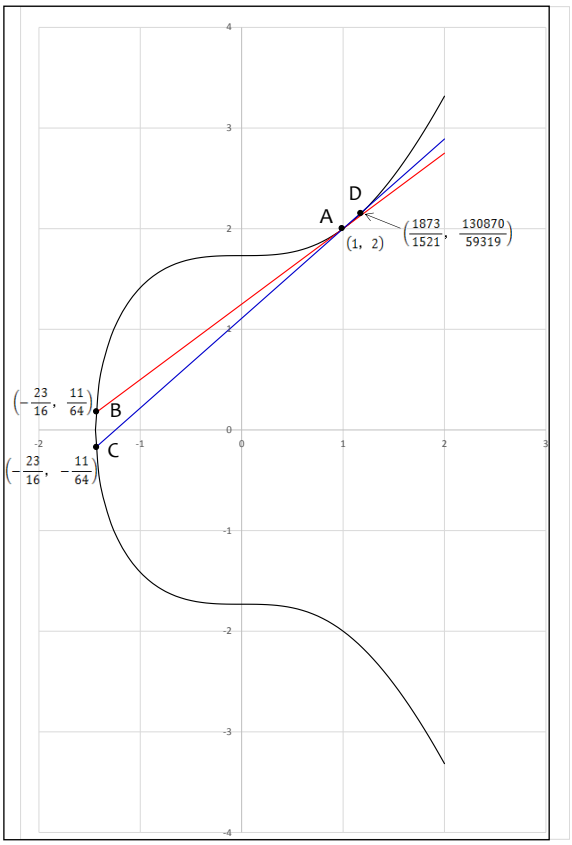
図Ｄにおいて、Ｅの有理点Ａ $(1,\ 2)$ における接線の方程式は、

$y=\frac{3}{4}x+\frac{5}{4}$ となる。この接線とEの交点を求めると、

有理点B$\left(-\frac{23}{16},\ \frac{11}{64}\right)$が得られる。

点Bの X 軸に対する対称点C$\left(-\frac{23}{16},\ -\frac{11}{64}\right)$と点A $(1,\ 2)$

を結ぶ直線 $y=\frac{139}{156}x+\frac{173}{156}$ とEの交点を求めると、点Dが得られ、これも有理点 $\left(\frac{1873}{1521},\ \frac{130870}{59319}\right)$ である。



図D 楕円曲線の群構造

この操作を繰り返し行うことにより、次々と有理点を計算することができ、すべての有理点を求めることができる。

これは、楕円曲線上の有理点が、群構造をなすためで、モーデルの定理として「有理数体上の楕円曲線の有理点全体は有限生成アーベル群をなす」ことが証明されている。

有限生成アーベル群【アーベル群とはその群における演算が可換である群】は、群の有限個の元 $(x_1,x_2,x_3,\cdots\cdots x_k)$ が存在して、その群のすべての元 x が $(n_1,n_2,n_3,\cdots\cdots n_k)$ を整数として、$x=n_1x_1+n_2x_2+\cdots\cdots+n_kx_k$ の形に書くことができることをいう。

（※７）「楕円曲線の加法公式、２倍公式」について

$P_1(x_1,y_1)$，$P_2(x_2,y_2)$ を楕円曲線 E：$y^2=x^3+ax+b$ 上の点とする。

$P_1\neq P_2$ のとき、$P_1+P_2=(x_3,y_3)$ とすると、(x_3,y_3) は直線 P_1P_2 とEの交点である。

直線 P_1P_2 の式は、$y-y_1=\frac{y_2-y_1}{x_2-x_1}(x-x_1)$ と表され、これをE：$y^2=x^3+ax+b$ に入れて

x について解くと、x_3 は次のようになる。

$$x_3=\frac{-x_1^3-x_2^3+x_1^2x_2+x_1x_2^2+y_1^2-2y_1y_2+y_2^2}{(x_2-x_1)^2}=\frac{-(x_1+x_2)(x_1^2-x_1x_2+x_2^2)+x_1x_2(x_1+x_2)+(y_2-y_1)^2}{(x_2-x_1)^2}$$

$$=\frac{-(x_1+x_2)(x_1^2-2x_1x_2+x_2^2)+(y_2-y_1)^2}{(x_2-x_1)^2}=\frac{-(x_1+x_2)(x_2-x_1)^2+(y_2-y_1)^2}{(x_2-x_1)^2}\quad\text{より、}$$

$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-(x_1+x_2)$，$y_3=\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)-y_1$ が求められる。

$P_1=P_2$ のとき、$P_1+P_2=2P=(x_3,y_3)$ とすると、

直線P_1P_2 は点P_1 における接線に一致するので、Eをx で微分して $2yy'=3x^2+a$，$y'=\frac{3x^2+a}{2y}$

よって、$P_1(x_1,y_1)$ における勾配は $y'=\frac{3x_1^2+a}{2y_1}$ である。従って、

$x_3=\left(\dfrac{3x_1^2+a}{2y_1}\right)^2-2x_1=\dfrac{x_1^4-2ax_1^2-8bx_1+a^2}{4(x_1^3+ax_1+b)}$ ， $y_3=\dfrac{3x_1^2+a}{2y_1}(x_1-x_3)-y_1$ が得られる。

E：$y^2=x^3+1$ のとき、$a=0,b=1$ とすると、$2P$ の x 座標は $\dfrac{x^4-8x}{4(x^3+1)}$ となる。

（※８）「複素数体上の楕円曲線」について

実数関数と同様に複素関数においてもテイラー展開が可能である。テイラー展開を負のべき乗まで拡張したものがローラン展開で、コーシーの積分公式を変形することによって得られ、点 a の近傍での展開は次式のように表される。

$$\boldsymbol{f}(z)=\cdots\cdots+\frac{a_3}{(z-a)^3}+\frac{a_2}{(z-a)^2}+\frac{a_1}{z-a}+a_0+a_1(z-a)+a_2(z-a)^2+a_3(z-a)^3+\cdots\cdots \qquad \cdots\cdots\cdots(イ)$$

ここで a_n は定数で、

$a_n=\dfrac{1}{2\pi i}\displaystyle\int_c \frac{f(w)}{(w-a)^{n+1}}dw$ によって与えられる。

(イ) 式において、$(z-a)^{-n}$ の項を主要部，$(z-a)^n$ の項を正則部という。

$\wp(z)$ を $z=0$ の近傍でローラン展開すると次式が得られる。

$$\wp(z)=\frac{1}{z^2}+\sum_{w\in L\neq 0}\left[\frac{1}{(z-w)^2}-\frac{1}{w^2}\right]=\frac{1}{z^2}+\left(3\sum_{w=1}^{\infty}\frac{1}{w^4}\right)z^2+\left(5\sum_{w=1}^{\infty}\frac{1}{w^6}\right)z^4+\cdots\cdots \qquad \cdots\cdots\cdots(ロ)$$

(ロ)は次のように導かれる。

$z=0$ での主要部は$\frac{1}{z^2}$ である。$\wp(z)$ は $z=w$に極を持ち$|z|<r$において $\boldsymbol{f}(z)=\wp(z)-\frac{1}{z^2}$ は正則である。

$\wp(z)$ は偶関数であるから$\boldsymbol{f}(z)$ も偶関数であり、$\boldsymbol{f}(z)$ のローラン展開は $|z|<r$において

$\boldsymbol{f}(z)=\wp(z)-\frac{1}{z^2}=\ c_0+c_2\,z^2+c_4\,z^4+c_6\,z^6+\cdots\cdots$と表され、係数$c_0$，$c_2$，$c_4$‥‥を求めると

$\boldsymbol{f}(z)=\displaystyle\sum_{w=1}^{\infty}\left[\frac{1}{(z-w)^2}-\frac{1}{w^2}\right]$ から、$f^{(2n)}(z)=\displaystyle\sum_{w=1}^{\infty}\frac{(2n+1)!}{(z-w)^{2(n+1)}}$ となる。

$z=0$ とすると、$c_0=\ \boldsymbol{f}(0)=0$，$\ c_{2n}=\dfrac{1}{(2n)!}f^{(2n)}(0)=\dfrac{1}{(2n)!}\displaystyle\sum_{w=1}^{\infty}\frac{(2n+1)!}{(-w)^{2(n+1)}}=\ (2n+1)\sum_{w=1}^{\infty}\frac{1}{w^{2(n+1)}}$

だから、$n=1$ とすると $c_2=3\displaystyle\sum_{w=1}^{\infty}\frac{1}{w^4}$ ， $n=2$ とすると $c_4=5\displaystyle\sum_{w=1}^{\infty}\frac{1}{w^6}$ となる。

従って $z=0$ の近傍では、

$\wp(z)=\dfrac{1}{z^2}+\left(3\displaystyle\sum_{w=1}^{\infty}\frac{1}{w^4}\right)z^2+\left(5\sum_{w=1}^{\infty}\frac{1}{w^6}\right)z^4+\cdots\cdots$ が導かれる。

一般にはc_2，c_4 の代わりに、ローラン係数から得られる量（$\wp$ 関数の不変量という）として

$g_2=20c_2=60\displaystyle\sum_{w=1}^{\infty}\frac{1}{w^4}$，$\ g_3=28c_4=140\displaystyle\sum_{w=1}^{\infty}\frac{1}{w^6}$ が用いられる。

$\wp$ 関数の不変量 g_2，$\ g_3$ を用いて $\wp(z)$ のローラン展開を表すと次のようになる。

$$\wp(z)=\frac{1}{z^2}+\frac{g_2}{20}\,z^2+\frac{g_3}{28}\,z^4\cdots\cdots \qquad \cdots\cdots\cdots\cdots(ハ)$$

（ハ）を微分すると、

$$\wp'(z)=-\frac{2}{z^3}+\frac{g_2}{10}z+\frac{g_3}{7}\,z^3\cdots\cdots \qquad \cdots\cdots\cdots\cdots(ニ)$$

次に $\mathrm{w}=\wp(z)$ が $\wp'(z)^2=4w^3-g_2\mathrm{w}-g_3$ $\cdots\cdots\cdots\cdots(ホ)$

を満たすことを示す。

（ハ）を３乗すると、

$$\wp^3(z)=\left(\frac{1}{z^2}\right)^3+3\left(\frac{1}{z^2}\right)^2\left(\frac{g_2}{20}\,z^2\right)+3\left(\frac{1}{z^2}\right)^2\left(\frac{g_3}{28}\,z^4\right)+\cdots\cdots$$

（$z^n(n\leqq 0)$の項はこの３項のみで、$z^n(n\geqq 0)$の項は無視できる）

$$\wp^3(z)=\frac{1}{z^6}+\frac{3g_2}{20}\frac{1}{z^2}+\frac{3g_3}{28}+\cdots\cdots \qquad \cdots\cdots\cdots\cdots(ヘ)$$

（ニ）を２乗すると、

$$\wp'^2(z)=\left(-\frac{2}{z^3}\right)^2+2\left(-\frac{2}{z^3}\right)\left(\frac{g_2}{10}z\right)+2\left(-\frac{2}{z^3}\right)\left(\frac{g_3}{7}\,z^3\right)+\cdots\cdots$$

（$z^n(n\leqq 0)$の項はこの３項のみで、$z^n(n\geqq 0)$の項は無視できる）

$$\wp'^2(z)=\frac{4}{z^6}-\frac{2g_2}{5}\frac{1}{z^2}-\frac{4g_3}{7}+\cdots\cdots \qquad \cdots\cdots\cdots\cdots(ト)$$

$\wp(z)=\wp'^2(z)-\left[4\wp^3(z)-g_2\wp(z)-g_3\right]$ に（ハ）（ヘ）（ト）を入れると、

$$\wp(z)=\left[\frac{4}{z^6}-\frac{2g_2}{5}\frac{1}{z^2}-\frac{4g_3}{7}+\cdots\right]-4\left[\frac{1}{z^6}+\frac{3g_2}{20}\frac{1}{z^2}+\frac{3g_3}{28}+\cdots\right]-g_2\left[\frac{1}{z^2}+\frac{g_2}{20}\,z^2+\frac{g_3}{28}\,z^4\cdots\right]-g_3$$

$$=\left(-\frac{2g_2}{5}-\frac{3g_2}{5}+g_2\right)\frac{1}{z^2}+\left(-\frac{4g_3}{7}-\frac{3g_3}{7}+g_3\right)+\left(-\frac{{g_2}^2}{20}z^2-\frac{g_2g_3}{28}\,z^4+\cdots\right)$$

より、第１項（$\frac{1}{z^2}$の項）と第２項（定数項）は０となり、$\wp(z)$ は z^2 以上の項のみを持つ整関数である。ここで、リュービルの定理（$\boldsymbol{C}$ 上有界な正則関数は定数関数のみである）から、$\wp(z)$ は定数である。

一方、右辺は z^2 以上の項しか存在しないので右辺＝０となり、

$\mathrm{w}=\wp(z)$ は、$\wp'(z)^2=4w^3-g_2\mathrm{w}-g_3$ が成り立つことが導かれた。

（※９）「保型形式」について

保型形式とはその名のとおり「型が保たれる」ということで、

$z\mapsto\left(\frac{az+b}{cz+d}\right)$ という変換に対し、$\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|a,b,c,d\in\boldsymbol{Z},ad-bc=1\right\}$ を満たすものについて型が保たれということを意味している。

$\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|a,b,c,d\in\boldsymbol{Z},ad-bc=1\right\}$ は、$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{SL}(2,\boldsymbol{Z})$ とも書かれ、$\mathrm{SL}(2,\boldsymbol{Z})$ は成分が整数の２次正方行列のことをいう。

$q=e^{2\pi iz}$ の変形により、複素上半平面Hの点 z に対応し、$|q|<1\leftrightarrow I_m(z)=y>0$ の同値が成り立つこ

と、そしてこの対応がD$(|q|<1$ を満たす単位複素円盤上の点$)$から、

$\Gamma_\infty/H=\left\{z=x+iy\in H\,\middle|\,-\frac{1}{2}<x\leq\frac{1}{2}\,,y>0\right\}$ への全単射（１対１写像）である。

変数 q のままで考えることと、変数 z に変換して考えることとの間に本質的な違いはなく、

z で表記すると、群の作用が１次分数変換 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot z=\dfrac{az+b}{cz+d}\ (z\in H)$ ……(チ)

と表され見やすいという利点があるので、以下 q をz に変換して記述する。

保型形式の代表的な例として、ラマヌジャンの Δ 関数がある。

ラマヌジャンの関数 $f(q)$ を$q=e^{2\pi iz}$ の置き換えで z の関数とみなし、$f(q)=\Delta(z)$ とおく。

$q=e^{2\pi iz}$ から $\Delta(z+1)=\Delta(z)$ が成り立ち、さらに$\Delta\left(-\dfrac{1}{z}\right)=z^{12}\Delta(z)$が成り立つ。これらの式は、

$SL(2,\ \boldsymbol{Z})$ の元、$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ と $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ の作用に関する変換式に対応している。すなわち、

$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}z=z+1,\ \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}z=-\dfrac{1}{z}$ であり、$\Delta(z+1)=\Delta(z)$ と $\Delta\left(-\dfrac{1}{z}\right)=z^{12}\Delta(z)$の２式は、

$\Delta\left(\dfrac{az+b}{cz+d}\right)=(cz+d)^{12}\,\Delta(z)$ の形にまとめることができる。

群 $SL(2,\ \boldsymbol{Z})$ は、$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ と $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ の２元で生成され、このことから任意の$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\ \boldsymbol{Z})$ に対し

$\Delta\left(\dfrac{az+b}{cz+d}\right)=(cz+d)^{12}\,\Delta(z)$ が成り立つことがわかる。

そこで、一般に任意の $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\ \boldsymbol{Z})$ に対し、$u\left(\dfrac{az+b}{cz+d}\right)=(cz+d)^{\mathrm{k}}\,u(z)$ が成り立つような関数 $u:H\to\boldsymbol{C}$ を $SL(2,\ \boldsymbol{Z})$ に関する重さk の保型形式という。u が正則関数であれば正則保型形式という。

$z\longmapsto\dfrac{az+b}{cz+d}$ によって関数が不変であるが、本当に不変なのは $k=0$ の場合のみで、それ以外の時は $(cz+d)^{\mathrm{k}}$ の分だけずれが生じているかのように見える。$(cz+d)^{\mathrm{k}}$ を保型因子というが、ずれが生じる理由は u をH の関数とみなしているためで、本来 u はリー群 $SL(2,\ \boldsymbol{R})$ 上の関数とみなすべきである。

$SL(2,\ \boldsymbol{R})$ はHに１次分数変換で作用するが、この作用で$\sqrt{-1}\in$ H を固定する行列は、回転行列

$\begin{pmatrix}cos\theta & -sin\theta\\ sin\theta & cos\theta\end{pmatrix}$ の形をした行列である。

$$\begin{pmatrix}cos\theta & -sin\theta\\ sin\theta & cos\theta\end{pmatrix}\cdot\sqrt{-1}=\frac{\sqrt{-1}\,cos\theta+(-sin\theta)}{\sqrt{-1}\,sin\theta+cos\theta}=\frac{\left[\sqrt{-1}\,cos\theta+(-sin\theta)\right]\left[-\sqrt{-1}\,sin\theta+cos\theta\right]}{\left[\sqrt{-1}\,sin\theta+cos\theta\right]\left[-\sqrt{-1}\,sin\theta+cos\theta\right]}$$

$$=\frac{\sqrt{-1}\,(sin^2\theta+cos^2\theta)}{(sin^2\theta+cos^2\theta}=\sqrt{-1}$$

となり、回転行列は$\sqrt{-1}$ を固定する。（逆に$\sqrt{-1}$ を固定する行列は回転行列に限られる）

$\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\ \boldsymbol{R})\middle|\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\sqrt{-1}=\sqrt{-1}\right\}=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\ \boldsymbol{R})\middle|\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\boldsymbol{O}(2)\right\}$ これより、

$SL(2,\ \boldsymbol{R})/SO(2) \cong \mathrm{H} \qquad g\cdot SO(2) \leftrightarrow g(\sqrt{-1})$

が成り立つ。これは解析的同型であり、H に双曲距離を入れ $SL(2,\ \boldsymbol{R})$ にリー群としての距離を入れた場合に、両者が距離空間として同型になる。（連続性や微分可能性も完全に一致する）このようにして、U を $\boldsymbol{G} = SL(2,\ \boldsymbol{R})$ 上の関数とみなしたものをφ と置くと、$\boldsymbol{u}(z) = \varphi(\mathrm{gk})$ $[\boldsymbol{K} = SO(2)]$ である。

$\boldsymbol{K}$ はリー群 $\boldsymbol{G}$ の極大コンパクト部分群である。

ずれ、$(cz+d)^{\mathrm{k}}$ は $\boldsymbol{u}$ をH 上ではなく $\boldsymbol{G}$ 上の関数とみなした時の $\boldsymbol{K}$ 成分の寄与からくる。

（※１０）「導手」について

Ｅを $\boldsymbol{Q}$ 上の楕円曲線とするとき、

$N(\mathrm{E}) = \prod_{p:\text{素数}} p^{f_p(E)}$ をＥの導手という。ここで $f_p(E)$ は、

・Ｅが p で良い還元を持つとき　$f_p(E) = 0$

・Ｅが p で乗法的還元を持つとき $f_p(E) = 1$

・Ｅが p で加法的還元を持つとき $f_p(E) = 2 + \delta_p$　$p \neq 2,3$ ならば $\delta_p = 0$ である。

以上から導手は、① $\Delta(\mathrm{E})$を計算し，その素因子の集合を B_E とする

② 各 $p \in B_E$ に対し c_4 を計算する事で$f_p(E)$ を計算する

③ $p^{f_p(E)}$ を全て掛け合わせる

という３つのステップで計算できる。

導手はＥが良い還元を持たないような素数すべての積であり、判別式が「悪い素数のリスト」を与えていたのに対し、導手は「悪い素数のリスト＋還元の様子」を明らかにするものである。

有理数体上の楕円曲線や上半平面上の保型形式には導手があり、小さい方から 11, 14, 15, 17, 19, ‥‥ となっている。

導手が 11 の楕円曲線は、上半平面上の保型形式

$q\prod_{n=1}^{\infty}\{(1-q^n)(1-q^{11n})\}^2 \quad q = e^{2\pi iz}$ にゼータ関数が一致する。

有理数体上の楕円曲線と上半平面上の重み２の保型形式のゼータ関数が一致するなら、両者の導手は一致する。もし、フライの楕円曲線の導手が、10 以下というようなことがあれば、矛盾があることになりフェルマー予想が証明される。

（※１１）「ヘッケ作用素」について

２次のオイラー積の代表的な例としてラマヌジャンのＬ関数 : $L(s,\ \tau)$ があるが、それ以外にはラプラシアンの固有関数 $\boldsymbol{u}(z)$ から得られるものがある。

基本領域上の関数 $\boldsymbol{u}$ の中でも特にラプアシアン、$\Delta = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$ の固有関数に着目する。

このような関数 $\boldsymbol{u}$ をマース波動形式と呼ぶ。（アイゼンシュタイン級数$E(z,\ \mathrm{s})$ はマース波動形式の例）ただし、$E(z,\ \mathrm{s})$ は$SL(2,\ \boldsymbol{Z})$ の基本領域上、連続スペクトルに対する固有関数の類似であるが、ここでは離散的な固有値に対する固有関数を対象とする。

ラプラシアンの固有関数 $\boldsymbol{u}(z)$ のフーリエ展開は一般に$z \mapsto z+1$ でなく$(x,y) \mapsto (x+1,y)$ であり、

$\boldsymbol{u}(z)=\sum_{\boldsymbol{n}=-\infty}^{\infty}a(n,y)e^{2\pi inx}$ の形となる。ラプラシアンの固有方程式から$a(n,y)$を求めると、

$a(n,y)=a(n)\sqrt{y}K_{s-\frac{1}{2}}(2\pi|n|y)$ よりフーリエ展開、$\boldsymbol{u}(z)=\sum_{n\in\boldsymbol{z}-(0)}a(n)\sqrt{y}K_{s-\frac{1}{2}}(2\pi|n|y)e^{2\pi inx}$

ここで、$K_s(y)$はKベッセル関数であり、$K_s(y)=\frac{1}{2}\int_0^{\infty}e^{-y\frac{t+t^{-1}}{2}}t^s\frac{dt}{t}$ を用いて$F(y)=\sqrt{\frac{2y}{\pi}}K_{s-\frac{1}{2}}(y)$

と表される。また、$K_{s-\frac{1}{2}}$のsは$\boldsymbol{u}$に付随するラプラシアンの固有値λから$\lambda=s(1-s)$として得られる複素数である。$\lambda=s(1-s)$のsをさらに$s=\frac{1}{2}+ir$によってrに変数変換すると、マース波動形式のフーリエ展開は

$$\boldsymbol{u}(z)=\sum_{n\in\boldsymbol{z}-(0)}a(n)\sqrt{y}K_{ir}(2\pi|n|y)e^{2\pi inx} \qquad \cdots\cdots\cdots\cdots(\text{ﾘ})$$

ここで、$\boldsymbol{u}$からなる固有空間の基底が存在することを示す。これは、すべてのマース波動形式$\boldsymbol{u}$に対して$L(s,\ u)$がオイラー積を持つわけではないので、$L(s,\ u)$がオイラー積を持つような$\boldsymbol{u}$で固有空間を張ることができるのか？固有空間の基底で$L(s,\ u)$がオイラー積を持つような$\boldsymbol{u}$からなるものが選べるか？を確認するためである。ここで、ヘッケ作用素が登場する。

任意の自然数mに対してヘッケ作用素数$T(m)$を定義し、$\boldsymbol{u}$が$T(m)$の固有関数であることが、$\boldsymbol{u}$のm番目のフーリエ係数に関する乗法性が成り立つことと同値であることを示す。

ラプラシアンや「ι」はすべての$T(m)$と可換であることからそれらすべての作用素の同時固有関数であるような$\boldsymbol{u}$を選べば、フーリエ係数は乗法的となり$L(s,\ u)$がオイラー積を持つ。

ヘッケ作用素の定義は次の式で与えられる。

$$(T(m)u)(z)=\frac{1}{\sqrt{m}}\sum_{ad=m}\sum_{b=0}^{d-1}u\left(\frac{az+b}{d}\right) \qquad \cdots\cdots\cdots\cdots(\text{ﾇ})$$

ここで$\sum_{ad=m}$は、$ad=m$をみたすような自然数の組(a,d)にわたる和を示す。

$m=p$ のとき、$(a,d)=(1,p)$，$(a,d)=(p,1)$ の２通りあり、$(a,d)=(1,p)$のときは$b=0,1,2$ ----- , p − 1で、$(a,d)=(p,1)$のときは$b=0$のみとなるので、

$(T(p)\boldsymbol{u})(z)=\frac{1}{\sqrt{p}}\left(\sum_{b=0}^{p-1}u\left(\frac{z+b}{p}\right)+\boldsymbol{u}(pz)\right)$ となる。

モーデル作用素の定義は、

$(T(p)\Delta)(z)=\frac{1}{p}\left(\sum_{l=0}^{p-1}\Delta\left(\frac{z+l}{p}\right)+p''\Delta(pz)\right)$ なので、係数は少し異なるが構造はまったく同じである。

この式を構成して、$T(p)\Delta=\tau(p)\Delta$（つまり Δ は$T(p)$ に対して固有値 $\tau(p)$ を持つ固有関数）が成り立つことから導かれた。ワイルズはモーデル作用素をヘッケ作用素に拡張し、作用素 $T(p)$ たちの作る重要な環（ヘッケ環）を導いた。すなわちマース波動形式に対するヘッケ作用素は、ラマヌジャンの Δ 関数に

対して定義されたモーデル作用素の一般化と考えられる。

ヘッケ作用素 $T(m)$ は次の乗法的な公式を満たす。

$$T(m)\,T(n)=\sum_{d/(m,n)} T\left(\frac{mn}{d^2}\right)$$

ここで $T(m)\,T(n)$ は互いに素な整数の組 (m,n) に対する乗法性を意味し、d は (m,n) の約数の全体を渡り、(m,n) は mとn の最大公約数を示す。

マース波動形式 $\boldsymbol{u}(z)$ がヘッケ作用素 $T(p)$（pは素数）の固有関数であるとし、$\boldsymbol{u}(z)$ はフーリエ展開が式（ﾘ）で与えられるとき、

$(T(p)\boldsymbol{u})(z)=a(p)\boldsymbol{u}(z)$ である。即ちヘッケ作用素 $T(p)$ の固有値は $a(p)$ に等しい。

参考文献

１．数論Ⅰ　Fermat の夢と類体論（加藤和也・黒川信重・齋藤毅）

２．数論Ⅱ　岩澤理論と保型形式（黒川信重・栗原将人・齋藤毅）

３．岩波講座　現代数学の展開　Fermat 予想１（齋藤毅）

８６「ＡＢＣ予想について」で触れたように、ＡＢＣ予想が正しければ、フェルマー予想は次のように簡単に証明されてしまう。

フェルマー予想の証明

n を 3 以上の自然数として、$x^n+y^n=z^n$ を満たす自然数の組 $(x,\ y,\ z)$ が存在したと仮定する。このとき$(x^n,\ y^n,\ z^n)$ は（$x,\ y$ はそれぞれ素数と考えてよいので）ＡＢＣトリプルとなる。

よって、$z^n<rad(x^ny^nz^n)^2$ であるが、根基の定義から $rad(x^ny^nz^n)^2=rad(xyz)^2$ であり、$x,\ y<z$ だから、$rad(xyz)^2\le(xyz)^2<(z^3)^2=z^6$ となる。よって、$z^n<z^6$ である。これは自然数 n が 6 より小さいことを示しているが、n は 3 以上だったので、n の可能性は 3，4，5 しかないことになる。

$n=3,\ 4,\ 5$ の場合は、すでに成り立たないことが個別に証明されているので「$x^n+y^n=z^n$ を満たす自然数の組 $(x,\ y,\ z)$ が存在する」とした仮定が誤りである。以上より、フェルマー予想が証明された。

（２０２１．０１．２５）