楕円曲線とモジュラー形式

Elliptic curves and modular form

楕円曲線が少ないという概念は、楕円曲線の全体からなる「楕円曲線のモジュライ空間 *moduli space* と呼ばれる集合を理解して初めて成立する。
モジュライ空間は、楕円曲線の集合に、ある数学的な解釈をいれたものである。したがって、それを理解するためには、まず楕円曲線を理解する必要がある。そして、その前に、数学における図形という概念を理解する必要がある。楕円曲線も、またその全体集合であるモジュライ空間も、現代数学においては１つの図形（多様体）とみなされる。そして、それらは、いずれも、ある空間に群が作用したときの基本群 *fundamental group* とみなされるのである。

１．基本領域

数学で用いられる図形の基本的な見方に、普遍被覆空間 *universal covering space*を基本群で割ったものとして図形を解釈する方法がある。

2 次元トーラスを例にとる。2 次元トーラスは、*xy* 平面 $\boldsymbol{R}^2$ に次の操作を施して得られる図形である。平面上の平行移動は 2 次元ベクトルに沿った動きとみなされるから、平行移動の全体は、$\boldsymbol{R}^2 = \{(x, y) \mid x, y \in \boldsymbol{R}\}$ と表されるが、このうち、*x, y* が共に整数であるような平行移動からなる部分集合 $\boldsymbol{Z}^2 = \{(x, y) \mid x, y \in \boldsymbol{Z}\}$ を考える。$\boldsymbol{Z}^2$ の元による平行移動で、平面上の点は、各座標の整数部分のみが変化し、少数部分は変わらない。逆に、座標の少数部分が等しいような点どうしは、$\boldsymbol{Z}^2$ による平行移動で移りあう。適当な $\boldsymbol{Z}^2$ の平行移動を施すことにより、平面上のどんな点も整数部分を 0 に揃えることができる。整数部分が 0 であるような座標からなる点のなす単位正方形 $I = \{(x, y) \mid 0 \leqq x < 1, 0 \leqq y < 1\}$ を $\boldsymbol{Z}^2$ で移すと平面全体が覆われ、しかもこの単位正方形 *I* 内の点どうしは互いに移りあわない。このような性質をもつ領域を、$\boldsymbol{Z}^2$ の基本領域という。*I* は、$\boldsymbol{Z}^2$ の平行四辺形などでも基本領域を表すことができる。

さて、Iの境界の 4 辺のうち、x, y 両軸上にある 2 辺は I に含まれるが、$x = 1, y = 1$ 上の 2 辺は含まれない。この 2 辺は、x, y 軸上の 2 辺と同一視される。したがって、基本領域を 1 つの曲面としてみると、下図のようなトーラ *torus* になる。これを 2 次元トーラス $\boldsymbol{T}$ と書く。

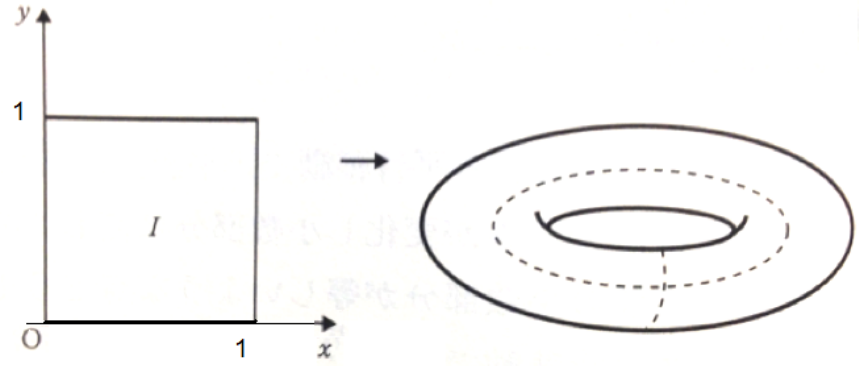

図 1

T の構成法をもう一度整理する。平面 $\boldsymbol{R}^2$ に、整数を成分に持つ 2 次元ベクトル $\boldsymbol{Z}^2$ が平行移動として作用している。すなわち、平面上の点$(x, y) \in \boldsymbol{R}^2$ に対し、平行移動 $(m, n) \in \boldsymbol{Z}^2$ が、$(m, n) \cdot (x, y) = (x + m, y + n)$と作用している。「・」は、作用点を意味する。$T$は、この作用で移りあう平面上の点どうしを同一視して得られる集合である。この T を「$\boldsymbol{R}^2$ における $\boldsymbol{Z}^2$ の基本領域」という。あるいは「$\boldsymbol{R}^2$ を $\boldsymbol{Z}^2$ で割った集合」という。記号で書くと、
$T = \boldsymbol{Z}^2 \backslash \boldsymbol{R}^2$ と書く。
円周 S^1 の場合には、$S^1 = \boldsymbol{Z} \backslash \boldsymbol{R}$
さらに、もう 1 つの例として、上で述べた $\boldsymbol{R}$ の代わりに複素平面 $\boldsymbol{C}$ を用いることが出来る。$\boldsymbol{C}$ と $\boldsymbol{R}^2$ は外見上同じになるはずだ。それらで割ってできる図形も同じ外見になるはずだ。R^2 に作用していた $\boldsymbol{Z}^2$ と同じように $\boldsymbol{C}$ に作用するのは、ガウスの整数環 $Z[\sqrt{-1}] = [x + yi \mid x, y \in \boldsymbol{Z}]$となる。したがって、先ほどのトーラス $\boldsymbol{T}$ は、$\boldsymbol{T} = \boldsymbol{Z}[\sqrt{-1}] \backslash \boldsymbol{C}$ **と表すことができる。**
当然、$\boldsymbol{C}$ と $\boldsymbol{R}^2$ は、中身の異なる集合であるから、各々の T は異なる元で構成されているが、それらの違いは虚数（すなわち自分自身とかけて負になるような数）を含むかどうかという点のみであり、足し算のみを考えている間は、両者は完全に同一のものとみなせる。数学的にいうと、$\boldsymbol{C}$ と $\boldsymbol{R}^2$ は加法部分群として同型となる。そして基本領域である $\boldsymbol{Z}[\sqrt{-1}] \backslash \boldsymbol{C}$ と $Z \backslash \boldsymbol{R}^2$ は、多様体として同型となり、上ではそれらを共通の記号 $\boldsymbol{T}$ で表したことになる。

２．双曲空間とモジュラー群

双曲平面 *hyperbolic plane* という日常生活から見ると少し変わった空間を解説する。そこに作用する基本群として、整数の代わりに、整数を成分をする行列を考える。これをモジュラー群 *modular group* という。

双曲平面の定義

複素平面の上側半分であり、複素上半平面と呼ばれる。

$H = \{x + iy \in \boldsymbol{C} \mid y > 0\}$ (複素上反平面)

これは単に複素平面を半分に切った形だが、実は、H 上の 2 点 z, w 間の距離を

$$d(z,w)=\log \frac{|z-\varpi| + |z-w|}{|z-\varpi| - |z-w|}$$

で定義する点が新しい。この新しい距離を双曲距離 *hyperbolic distance* という。双曲距離を導入することで、直線の概念も新しくなる。もともと直線とは、2点間を結ぶ最短径路だったから、距離の測り方が変われば最短径路も変わる。双曲線距離で2点間$z, z' \in H$を結ぶ最短径路は、$z, z' \in H$を通り中心が実軸上にあるような円周となる。（ただし、$z, z' \in H$が縦に並んでいるとき、すなわち$Re(z) = Re(z')$のときは、$z, z' \in H$を結ぶ鉛直線が最短径路である。これは、中心が無限遠点にあるような半径∞の円周とみなせる。）これらの最短径路を表す曲線を測地線 *geodesics* という。測地線は直線の概念を拡張したものであり、通常のユークリッド空間に対しては直線を意味する。

さて、上で定義した距離 $d(z, w)$がどんな距離なのか、さらに説明する。そのために、正の実数上の単調増加函数

$$u(d) = \frac{\cosh d - 1}{2}$$

を考える。ただし、$\cosh d = (e^{d} + e^{-d}) / 2$ である。$u(d)\ (d>0)$ は、単調増加であるから、d の大小は $u(d)$の大小を見ればわかる。そこで、$u(d(z,w))$を実際に計算してみると、

$$u(d(z, w)) = \frac{|z-w|^2}{4\ Im(z)\ Im(w)}$$

となる。*Im* は、複素数 *complex number* の虚部 *imaginary part* を表す記号である。これより 2 点間の距離
$d(z, w)$は、x 軸の付近の虚部が小さいところでは見た目より短いように定義されていることがわかる。

一例として三角形を考えてみる。領域 *domain*
$D = [z \in H : 0 \leqq Re(z) \leqq 1/2, |z| > 1]$
は、3 っの境界がすべての測地線からなるから、H 内の三角形である。

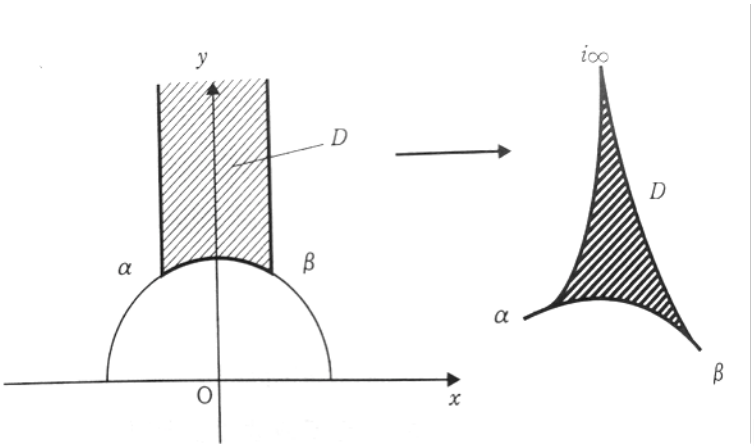

図 2

次に、H に作用する基本群 Γ を考える。考える対象は、
$\Gamma \subset SL(2, \boldsymbol{R})$, すなわち、$\Gamma$ は

$$SL(2, R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1 \quad a, b, c, d \in R \right\}$$

の部分群であるとする。$SL(2, R)$ は H に一次分数変換として作用する。この作用は、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

によって定義される。$Z \in H$ すなわち $Im(z) > 0$ のときに

$$\frac{az + b}{cz + d} \in H \text{ すなわち } Im\left(\frac{az + b}{cz + d}\right) > 0$$

となることは地道に計算すれば確かめられる。実際、$z = x + iy \ (y > 0)$とおくと、

$$Im\left(\frac{az+b}{cz+d}\right) = Im\left(\frac{(az+b)(cz+d)}{|cz+d|^2}\right)$$
$$= Im\left(\frac{(ax+b+ayi)(cx+d-cyi)}{|cz+d|^2}\right)$$
$$= \frac{-(ax+b)cy+ay(cx+d)}{|cz+d|^2}$$
$$= \frac{(ad-bc)y}{|cz+d|^2} = \frac{y}{|cz+d|^2} > 0$$

である。この *SL(2,R)*の作用が、トーラスの例における ***R***^2 分だけの平行移動に相当する。したがって、***Z***^2 に相当するものとして、成分の実数 ***R*** を整数 ***Z*** に制限した。

$$\Gamma=SL(2,Z) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad-bc=1,\ a,\ b,\ c,\ d \in Z\right\}$$

を考える。これをモジュラー群という。

モジュラー群は、*H* に対して実際にどのように作用するのだろうか。少し具体例で見てみる。
先ず、元

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

に注目する。一次分数変換の式に当てはめてみると、この元は写像として

$$z \mapsto z+1$$

すなわち、上半平面で右側に 1 だけ平行移動する写像である。これより、横幅 1 の縦長領域を元

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

で何度も移せば、*H* 全体を覆う。
たとえば、*-1/2 < x ≦ 1/2* と定めれば、下図のようになる。

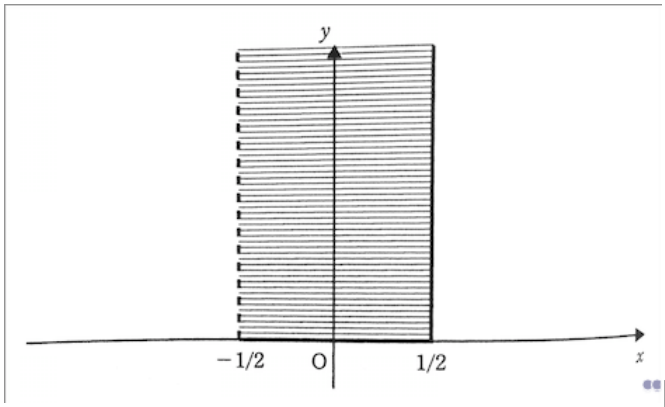

図 3

上半面のどの点も、必ずこの範囲内の点に Γ の元で移ることができる。次に元

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \Gamma$$

に注目する。一次分数変換の式に当てはめると、この元は写像として、

$$z \mapsto -\frac{1}{z}$$

となる。この写像は絶対値が 1 より大きい元と小さい元を入れ替える働きをしているから、単位円周の内部と外部を入れ替える写像である。たとえば、単位円の外側の領域は、

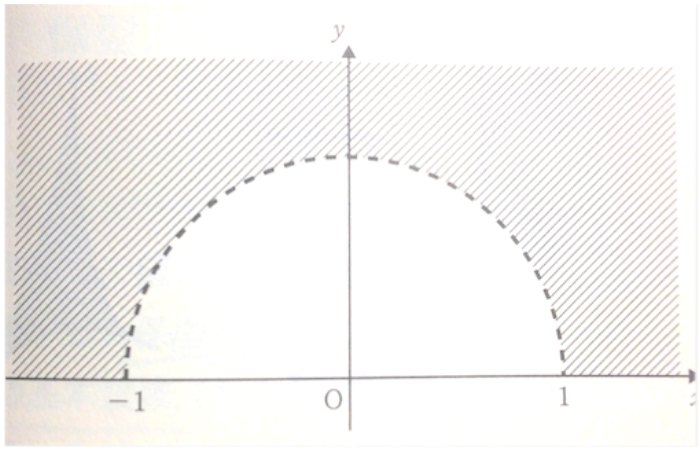

図 4

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \Gamma$$

によって全体を覆う。

以上のことから、前図 $(-1/2 < x \leqq 1/2)$ と上図(単位円周の外部)の共通部分の領

域は、モジュラー群Γの作用で H 全体を覆うことがわかる。実際この領域が Γ の基本領域となっている。式で書くと、次のようになる。

$$\Gamma\backslash H = \left\{ z=x+iy \in H:\ -\frac{1}{2} < x \leq \frac{1}{2},\ |z|>1 \right\}$$

$$\cup \left\{ z=x+iy \in H:\ |z|=1,\ 0 \leq x \leq \frac{1}{2} \right\}$$

これを図示したのが下図である。この基本領域は双曲平面における“三角形”であり、通常の距離感覚に会うように描き直すと、右側の図のように無限遠点 *point at infinity* で先細りの“袋”になる。

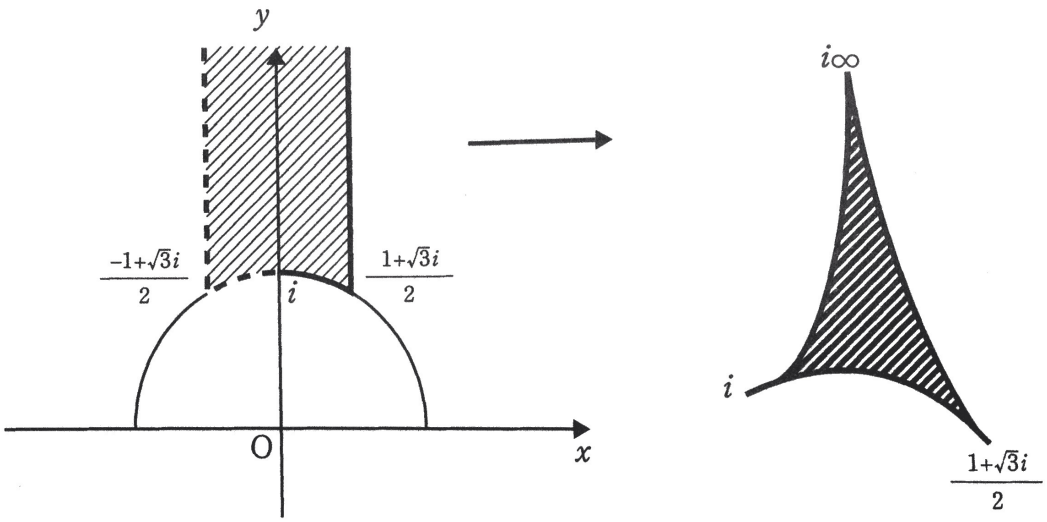

図 5

３．保型形式の古典理論

望月論文の理解に必要な保型形式の理論を概観する。保型形式とは、前説で解析したモジュラー群の基本領域（たとえば前図の三角形）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規則にしたがっている関数のことである。

ここで、「ある規則」とは、整数 k を用いて表され、モジューラー群 $\Gamma = SL(2, \mathbf{Z})$ の任意の元 $\gamma \in \Gamma$ に対し、$f(\gamma \cdot z) = (cz + d)^k f(z)$ $(z \in H)$ を満たすことである。黒点・は前説で登場した一次分数変換の作用を表す。このような規則を満たしながら、上半平面 H 全体上で定義される関数 $f(z)$ を、重さ

weight k の保型形式と呼ぶ。
z は複素数だから、*f(z)*は複素関数であり、実数上の関数のようにグラフが目で見える形で描けるわけではないが、実数のときに微分可能と呼んでいた「関数が滑らか *smooth* である」ことに相当する概念は、複素数上でも正則と呼ばれる概念として存在している。

したがって、保型形式にも *f(z)*として正則関数 *holomorphic function* と非正則関数があり得るが、ここで登場するのはもっぱら正則保型形式のみとする。以下、保型形式といえば正則保型形式を指すものとする。すなわち、*f(z)*が上半平面 *H* 上で正則であるような場合だけを考える。
保型形式の例として、まず挙げられるのが、アイゼンシュタイン級数である。アイゼンシュタイン級数は、保型形式すなわち上半平面上の関数でありながら、同時に、複素平面内の「格子 *lattice* の関数」とみなすこともできる。この第二の見方は重要であり、モジュライ空間の理解に欠かせない。そこでこの冊子ではアイゼンシュタイン級数を、格子の関数として導入していく。
$\Omega = <\omega_1, \omega_2>$とは、一次独立な複素数の組$(\omega_1, \omega_2)$を用いて、
$\Omega = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$
と表される集合のことである。複素平面上で点が 2 次元的な広がりを持って並んでいる様子を思い浮かべればよい。

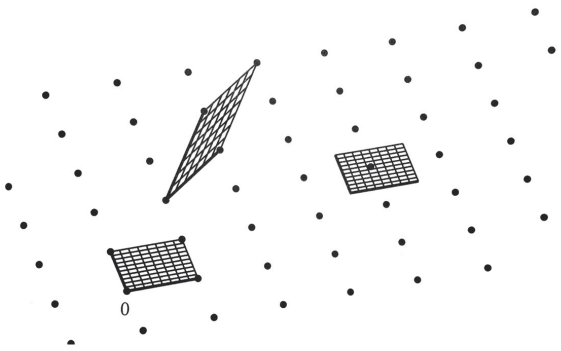

図 6

格子は複素平面内に離散的かつ周期的に分布しているので、ちょうど実数内に整数が分布している状況に似ており、いわば整数の複素版ともいえる。実際、ガウス整数の全体からなる集合 $|\sqrt{-1}|$ は格子の例であり、$\omega_1=1$, $\omega_2=\sqrt{-1}$ の場合である。

実数の場合に整数のべき乗の逆数の和をゼータ ζ として考えたが、その類似として、ここでも格子をなす点たちのべき乗の逆数の和を考えてみよう。

$$G_{2n}(\omega_1,\ w\omega_2) = \sum_{\omega\in\Omega-\{0\}} \frac{1}{\omega^{2n}}$$

指数を偶数 2n に限っているのは、奇数のときは ω と $-\omega$ の項どうしが打ち消しあって 0 になってしまうからである。自然数 n に対し、この級数は絶対収束する。
また定義式からすぐにわかるように、0 でない複素数 λ に対し、

$$\lambda^{2n}\ G_{2n}(\lambda\omega_1,\ \lambda\omega_2) = G_{2n}(\omega_1,\ \omega_2)$$

が成立する。そこで、G_{2n} の 2 つの変数のうち、$\omega_2 = 1$ に揃えたものを

$$G_{2n}(z,\ 1) = G^*_{2n}(z)$$

とおき、$G^*_{2n}(z)$ をアイゼンシュタイン級数と呼ぶ。$G^*_{2n}(z)$ を直接定義すれば、

$$G^*_{2n}(z) = \sum_{\substack{(m,n)\in z^2 \\ (m,\ n)\neq(0,\ 0)}} \frac{1}{(mz\ +\ n)^{2n}}$$

となる。
これが重さ *k=2* の保型形式であるかどうかを調べてみよう。
保型形式の定義

$$G^*_{2n}(\gamma.z) = (cz\ +\ d)^{2n}\ G_{2n}(z)$$

が成り立つかどうかをみればよいから、左辺を次のように変形してみる。

$$G^*_{2n}(\gamma.z) = G^*_{2n}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot\ z\right) = G^*_{2n}\left(\frac{az+b}{cz+d}\right)$$
$$= G_{2n}\left(\frac{az+b}{cz+d},\ 1\right) = (cz+d)^{2n} G_{2n}(az+b,\ cz+d)$$

ここで、関数 $G_{2n}(\omega_1,\ \omega_2)$ がもともと格子 Ω の関数であったことを思い出そう。

すなわち、1 つの格子 Ωに対して 2 つの表示 $\Omega=(\omega_1,\ \omega_2)$，$\Omega=(\omega'_1,\ \omega'_2)$ があるとき、

$$G_{2n}(\omega_1,\ \omega_2)\ =\ G_{2n}(\omega'_1,\ \omega'_2)$$

である。したがって、もし格子として、$<az+b,\ cz+d>=<z,\ 1>$が成り立てば、上の式に続けて

$$G^*_{2n}(\gamma.z)=(cz+d)^{2n}G_{2n}(az+b,\ \ cz+d)$$
$$=(cz+d)^{2n}G_{2n}(z,\ \ 1)=(cz+d)^{2n}G^*_{2n}(z)$$

となり、$G^*_{2n}(z)$ が重さ $2n$ の保型形式となる。実際にこれが成り立つのかどうかについて、次の**定理**が解答を与える。

定理 1

以下の 2 つの条件は同値である。

(A) 2 つの格子 $\Omega=<\omega_1,\ \omega_2>$，$\Omega=<\omega'_1,\ \omega'_2>$が同一の集合である。

(B) $\Gamma=SL(2,\ Z)$のある元 γ によって

$$\begin{pmatrix}\omega'_1\\ \omega'_2\end{pmatrix}=\gamma.\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\ \ or\ \ \begin{pmatrix}\omega'_1\\ \omega'_2\end{pmatrix}=\gamma.\begin{pmatrix}\omega_2\\ \omega_1\end{pmatrix}$$

と表される。

（証明は省略）

これより、$G^*_{2n}(z)$ と楕円曲線 *elliptic curves* や楕円関数 *elliptic function* の関わりを見て行く。はじめに注意しておくと、楕円曲線とは、楕円 *ellipse* という曲線ではない。楕円関数とは、二重周期関数、すなわち複素平面上の関数で格子 Ωに関して周期的であるような関数のことである。式で表すと、$f(z+\omega)=f(z)$が、格子 Ωの任意の複素数 z に対して常に成り立つような関数 $f(z)$を楕円関数という。楕円関数は格子の基本領域での値が決まれば、それを繰り返して全平面での値が決まる。仮に基本領域上で正則有界 *bounded regular* であるとすると、全平面でも正則有界となり、そんな関数は定数関数しかない。（これは複素関数論で

有名なリュービルの定理 *theorem of Liouville* である)。したがって、定数でない楕円関数は必ず値を持つ。
最も基本的な楕円関数は各格子点で 2 位の極を持つ関数であり、ワイエルシュトラウスのペー関数 pe-function と呼ばれる。定義は、各格子 Ω に対して、次のように与えられる。

$$\wp(z,\ \Omega) = \frac{1}{z^2} + \sum_{\omega\in\Omega-\{0\}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

この定義を初めて見たとき、奇異に感じるかもしれないが、もともと $z \mapsto z+\omega$ の変換で関数値が不変という性質は、すべての格子点 $\omega \in \Omega$ にわたる和を考えれば満たされるとの発想からきている。

$$\sum_{\omega\in\Omega}\frac{1}{(z-\omega)^2}$$

しかし、この和はこのままでは発散してしまう。なぜなら、この和を構成する各項 $\frac{1}{(z-\omega)^2}$ は ω の(-2)乗のオーダーであり、2 次元の格子 ω にわたって和をとれば、ちょうど、1 次元の格子に関する(-1) 乗の和と同じように発散する。

$$\sum_{n=1}^{\infty}\frac{1}{n}=\infty$$

そこで、(0 以外の $\omega \in \Omega$ に対して)各項から 1 /ω ^2 を引くことによる、ω の次数を下げて収束しやすくしたものが、上記のペー関数 $\wp(z,\ \Omega)$ である。
実に驚くべきことに、このペー関数が、先に見たアイゼンシュタイン級数を用いて表される。ペー関数のべき級数展開の係数がアイゼンシュタイン級数で書ける。その具体的な形を求めてみよう。以下格子 Ω を固定して考えるので、

$\wp(z,\ \Omega)=\wp(z)$ と略記する。

はじめに、|z|<|ω|すなわち|z/ω|<1 において、

$$\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}=\frac{1}{\omega^2}\left(\frac{1}{\left(1-\frac{z}{\omega}\right)^2}-1\right)$$

ここで、

$$\frac{1}{\left(1-\frac{z}{\omega}\right)^2}=\omega\left(\frac{1}{\left(1-\frac{z}{\omega}\right)}\right)'=\omega\left(\sum_{n=0}^{\infty}\left(\frac{z}{\omega}\right)^n\right)'=\omega\sum_{n=1}^{\infty}\frac{n}{\omega}\left(\frac{z}{\omega}\right)^{n-1}$$

$$=\sum_{n=1}^{\infty}\frac{nz^{n-1}}{\omega^{n-1}}=1+\sum_{n=2}^{\infty}\frac{nz^{n-1}}{\omega^{n-1}}=1+\frac{(n+1)z^n}{\omega^n}$$

であるから、

$$\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}=\frac{1}{\omega^2}\left(\frac{1}{\left(1-\frac{z}{\omega}\right)^2}-1\right)=\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}$$

となる。したがって、ペー関数の定義により

$$\wp(z)=\frac{1}{z^2}+\sum_{\omega\in\Omega-\{0\}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)=\frac{1}{z^2}+\sum_{\omega\in\Omega-\{0\}}\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}$$

となる。

ここで、各 n に対して $Z^{\wedge}2$ の係数を計算する。N が奇数のときは、$\omega\in\Omega$ に対して $-\omega\in\Omega$ であるから、和 $\Sigma_{\omega\in\Omega-\{0\}}$ において、そららの項が互いに打ち消しあって 0 になる。n が偶数のとき、$n=2k$ ($k=1,2,3,\ldots.$) とおくと、$z^{\wedge}2k$ の係数は、

$$\sum_{\omega\in\Omega-\{0\}}\frac{2k+1}{\omega^{2k+2}}=(2k+1)\sum_{\omega\in\Omega-\{0\}}\frac{1}{\omega^{2k+2}}=(2k+1)G_{2k+2}$$

となる。よって、$\wp(z)$ の $z=0$ のまわりのべき級数展開は、z の偶数乗のみからなり、正の偶数乗の係数は $(2k+1)G_{2k+2}\ \ (k=1,\ 2,\ 3,\ \ldots)$ となる。以上により、次の式が示された。

$$\wp(z)=\frac{1}{z^2}+\sum_{k=1}^{\infty}(2k+1)\,G_{2k+2}z^{2k}$$

$\wp(z)$ はもともと $z=0$(格子点)で 2 位の零点を持ち、それ以外の点で正則な関数であったが、このように展開式を明確に求めたことにより、$\wp(z)$ とその導関数 $\wp'(z)$ の関係式を次のように導くことができる。すなわち、展開式を具体的に書き下すと、

$$\wp(z)=z^{-2}+3G_4z^2+5G_6z^4+\ldots.$$

これを微分して 2 乗すると、

$$\wp'(z)^2=4z^{-6}-24G_4z^{-2}-80G_6+\cdots$$

この初項 $4z^{-6}$ を消すために、$\wp(z)^3$ を計算すると、

$$\wp(z)^3=z^{-6}+9G_4z^{-2}+15G_6+\cdots$$

となる。これより、関数

$$f(z) = \wp'(z)^2 -4\wp(z)^3+60G_4\wp(z)+140G_6$$

は、展開式において z の負べきの項がすべて消えるので正則になる。一方、$\wp(z)$ は楕円関数であったから、$\wp'(z),\ \wp^3(z)$ も二重周期を持ち、楕円関数であり、それらの組合わせである $f(z)$も楕円関数となる。よって、$f(z)$は全平面で正則な楕円関数だから、先ほど見たように定数となる。一方、$f(0)=0$ となることが容易にわかるので、この定数は 0 である。これにより $f(0)=0$, すなわち

$$\wp'(z)^2=4\wp(z)^3-60G_4\wp(z)-140G_6$$

が成り立つことがわかる。

$$g_2=60G_4,\quad g_3=140G_6$$

と略記すると、先ほどの関係式はより簡潔に

$$\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3$$

となる。これは、点 $(\wp(z),\ \wp'(z))$ が曲線

$$y^2=4x^3-g_2x-g_3$$

の上にあることを表している。$g_2,\ g_3$ は格子 Ωによって定まる定数であるから、この曲線も格子 Ωを与えるごとに決まる。この曲線こそが楕円曲線と呼ばれるものであるわけだが、ここで注意すべきは、今扱っている変数 $x=\wp(z),\ y=\wp'(z)$ はすべて複素数であるということだ。したがって「曲線」という用語が表す図形も、日常に描く図形の形状としてはむしろ曲線に近いものとなる、次節では

この辺りから解説していこう。

４．楕円曲線のモジュライ空間

楕円曲線は、abc 予想に関する望月論文や、テイラーとワイルズによるフェルマー予想の証明など、数論の進展において大きな役割を果たしている。本説では楕円曲線の意味を解説し、その全貌であるモジュライ空間 *moduli space* を把握しよう。

数学で曲線とは 1 次元多様体のことである。ここで次元とは、図形上の点を表すために必要な変数の個数のことだ。たとえば、前節に登場した図形

$$y^2=4x^3-g_2x-g_3$$

を曲線と呼んだ理由は、この図形上の点は、x を 1 つ定めるごとに、y は

$y=\pm\sqrt{4x^3-g_2x-g_3}$ と、高々2 つに特定される。したがって、この図形を

$y=\sqrt{4x^3-g_2x-g_3}$ と $y=-\sqrt{4x^3-g_2x-g_3}$ の 2 つの部分に分けると、各部分では 1 つの変数 x で図形上の点を特定できる。したがって、この図形上の点を特定できる。したがって、この図形は 1 次元である。

1 次元多様体は、xy 平面上に通常のイメージ通りの曲線のグラフとして表される。この視覚的な印象から曲線という用語が用いられるわけだが、実際にはこれが通常でいう曲線のイメージ(※日本語のイメージという言葉は感覚という意味)に合致するのは、x,y が実数の場合のみであるとに注意する必要がある。数論では、楕円曲線を用いる場合、x,y は複素数や p-進数 *p-adic number* など、実数以外となることが多い。

望月論文で用いられているのも x, y が複素数の場合である。このように、図形(多様体)の概念は、変数をどの集合で考えるかによって異なる。x, y を実数、複素数としたときの次元を「実数上の次元」「複素数上の次元」という。実数上であれ、複素数上であれ、1 次元のものを曲線というのである。

複素数は、もともと 1 つの変数が複素数平面の点として表される。複素平面の点は、実部と虚部という 2 つの実数で表されるから、複素平面そのものが、実数上では 2 次元多様体となる。したがって、x, y が複素数である場合の曲線すなわち、複素数上の 1 次元多様体は、実数上の 2 次元多様体となり、通常の感

覚でいえば曲線のイメージとなる。望月論文で用いられるモジュライ空間の理解には、x, y が複素数である場合の楕円曲線が必要となる。これは視覚的には曲線のイメージとなっていることに注意する必要がある。

以上を踏まえて、前節で登場した楕円曲線

$$y^2=4x^3-g_2x-g_3$$

の形状をみてみよう。
結論を先に述べると、楕円曲線の形状は最初の節で見たトーラスになる。ただし、$T=Z^2\setminus R^2$ あるいは $T=Z[\sqrt{-1}]\setminus C$ であったが、楕円曲線は格子 $Z[\sqrt{-1}]$ の代わりに楕円曲線の定義に用いた格子 Ω をとり、$\Omega\setminus C$ としたものである。$Z[\sqrt{-1}]$ は格子点が縦方向にまっすぐ並んでいるが、一般の格子は図 6 のように斜めに並んでおり、基本領域は正方形でなく平行四辺形になる。だが平行四辺形であっても向かい合う辺どうしを同一視すれば、正方形と同様にトーラスになる。そして、それが楕円曲線の形なのである。

すなわち、複素平面 C 内の任意の格子 Ω に対して定数 $g_2=g_2(\Omega),\ g_3=g_3(\Omega)$ を前述のようにおくとき、楕円曲線

$$E:\ y^2=4x^3-g\in g_3\ (x,\ y\in C)$$

は多様体としてトーラス $\Omega\setminus C$ と同型になるのだ。そして、どのようにしてこのような同型が成り立つのか、その中身を表すのが、ペー関数 *pe function* なのである。実際、この同型の対応は次のように与えられる。

定理２
次の対応は同型である。

$$\phi:\ \Omega\setminus C\ \to\ E$$
$$z\ \mapsto\ (\wp(z),\ \wp'(z))$$

以下、この事実を説明する。

任意の z に対して点 $(\vartheta(z),\ \wp'(z))$ が E 上にあることは、前節の末尾で見たので、

ここではまず、対応 ϕ が E 全体への一対一写像であることを説明しよう。
はじめに E 全体への写像となる理由を示すため、E の任意の点を $(x,\ y)$ とおき、これに対して $\phi(z)=(x, y)$ となる $z\in\Omega\setminus\boldsymbol{C}$ が必ず存在することを示す。
関数

$$f:\ \Omega\setminus\boldsymbol{C}\ \rightarrow\ \boldsymbol{C}$$
$$z\ \mapsto\ \wp(z)\ -\ x$$

を考える。(これは z の関数であり、x は定数とみなしている)。$f(z)$は、$\wp(z)$ と同じく楕円関数(二重周期関数)である。今、仮に $f(z)=0$ なる z が存在しないとすると、逆数をとった関数 $1/f(z)$は極を持たず有界となる。
$1/\ f(z)$ は楕円関数であるから、二重周期性によって、全複素平面上で正則 *non-singular* かつ有界となり、複素数論のリュービルの定理によって定数となってしまう。これは $f(z)$の定義に反する。よって背理法により、$f(z)=0$ すなわち $\wp(z)=x$ なる z が存在する。

この z について $\wp(z)^2=y^2$ が成り立つから、$\phi(z)=(x, y)$または $\phi(z)=(x,\ -y)$と

なる。前者の場合は z が求める解であり、後者の場合は $\wp(z)$ が偶関数で $\wp'(z)$ が奇関数であることに注意すると、$\phi(-z)=(x,y)$ が成り立つから、$-z$ が求める解である。
これで、対応する ϕ が E 全体への写像であることが示された。
次に、対応一対一写像であることを示す。基本領域内の点 z_1, z_2 に対し、$\phi(z_1)=\phi(z_2)$の仮定のもとで $z_1=z_2$ を示せばよい。
今度は、関数
$f(z)=\wp(z)-\wp(z_1)$

を考えると、$f(z)$は楕円関数であり、$z=z_2$ を零点に持つ。$\wp$ は偶関数だから $z=-z_1$ も零点である。さらに、仮定より $z=z_2$ も零点である。

これで $f(z)$の零点が 3 つ見つかったわけだが、$\wp$ は各基本領域内に 2 位の極を 1 個だけ持ち、それ以外の極はない。複素関数論によれば、有理型関数の極の位

数の総和は等しいので、今挙げた３つの零点のうち 2 つは同一でなくてはならない。
よって、次の３つのいずれか少なくとも１つが成り立つ。

（１）$z_1 = z_2$
（２）$z_1 = -z_2$
（３）$z_1 = -z_1$

（１）が成り立てば今の目標を達成する。

仮に（２）が成り立つとすると、$\wp'$ が奇関数であることから

$$\wp'(z_1)=\wp'(z_2)=\wp'(-z_1)= -\wp'(z_1)$$

となり、$2\wp'(z_1)=0$ より $\wp'(z_1)=0$ となってしまう。ところが、次の定理で示すように、$\wp'(z)=0$ の解 z はすべて求められており、いずれの場合も z と $-z$ は基本領域内の同じ点に対応する。したがって、（２）が成り立てば（１）が成り立つ。

次に、（３）が成り立つとすると、再び $\wp'$ が奇関数であることから

$$\wp'(z_1)=\wp'(-z_1)=-\wp'(z_1)$$

より $\wp'(z_1)=0$ であり、z_1 は $\wp'(z)=0$ の解だから、方程式 $\wp(z)-\wp(z_1)=0$ の重解となる。この方程式は z_1 を重根に持ち、かつ仮定により z_2 を解に持つ。解の位数の総計は 2 であるから、$z_1=z_2$ でなければならない。よってこの場合にも（１）が成り立つ。
以上、かなり込み入った議論があったが、これで対応 ϕ が一対一写像であることを示せた。

さて、点どうしが一対一に対応したからと言って、同じ形状とみなせるとは限らない。トーラスは滑らかであり尖っている箇所はないから、楕円曲線とトーラスが同型であると見るには、楕円曲線がトーラスと同様に滑らかであることを示す必要がある。

多様体が滑らかであることの一般的な定義はここでは述べないが、楕円曲線

$$E:\ y^2=4x^3-g_2x-g_3$$

の場合は、右辺の 3 次式が重根を持たなければならない滑らかである。このことは、x, y が実数の場合にグラフの形状を見れば、雰囲気が理解できるだろう。次の図では、上段に 3 次式が重根を持たない場合の例を 2 つと、下段に重根を持つ例を 1 つ挙げた。上段の左図は 3 つの実数解を持つ場合である。

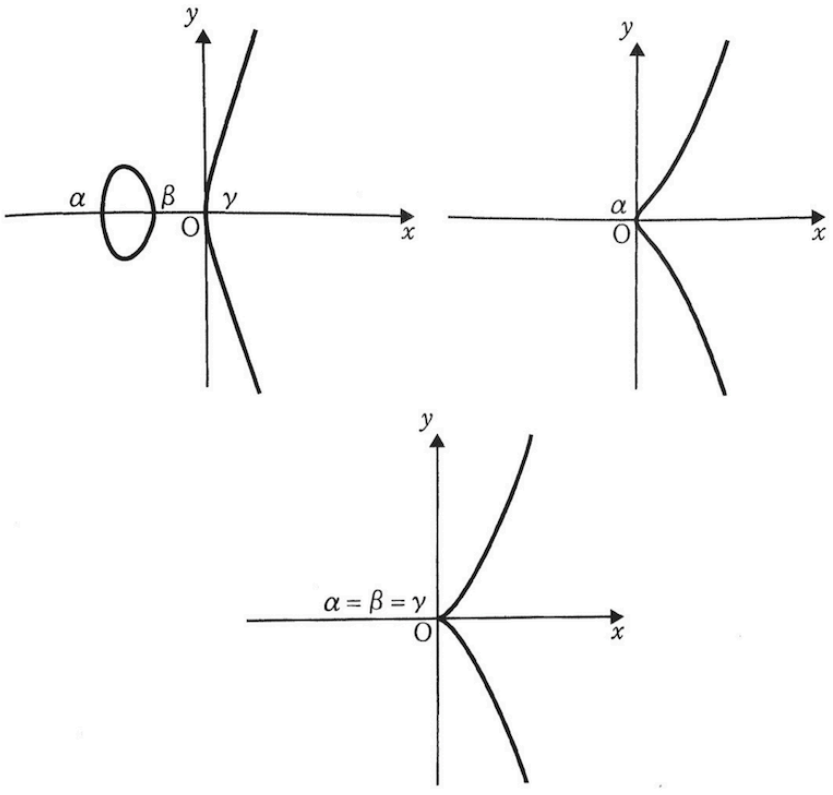

図 7

このとき、

$y=\pm\sqrt{4x^3-g_2x-g_3} = \pm\sqrt{4(x-\alpha)(x-\beta)(x-\gamma)}$ $(\alpha<\beta<\gamma)$ において、根号内が 0 以上になる範囲のみ y は存在するので、図のように $\alpha<\beta<\gamma$ のみでグラフは存在す

る。上段の右図は 1 つの実数解 α と、2 つの虚数解を持つ場合である。この場合はグラフは $\alpha \leqq x$ でのみ存在する。上段のいずれのグラフも曲線は滑らかである。一方、下段は原点において重解を持つ例である。虚数解は共益複素数と組になるので、重解は必ず 3 重解となることは直にわかる。図は原点で 3 重解を持つ。

$$y^2=4x^3$$

のグラフだが、このとき、原点においてグラフは尖って cusp いる。
以上の観察によって、楕円曲線が滑らかであることを確かめるには、右編の 3 次式が重根を持たないことを示せばよいことがわかった。この結論は、以下の定理によって示される。

定理３
人の格子 $\Omega \in C$ に対し、前述のように

$$g_2=g_2(\Omega),\quad g_3=g_3(\Omega)$$

とおくと、3 次方程式

$$4x^3-g_2x-g_3=0$$

は重根を持たない。すなわち、判別式

$$\triangle(\Omega)=g_2(\Omega)^3-27g_3(\Omega)^2$$

は 0 でない。

(証明省略)

楕円曲線の形状がトーラスであることがわかった。さて、ではいよいよ本冊子の目標である楕円曲線の全体の集合がどのような形をしているのか考えてみよう。

これまでの議論では、我々はまず格子 Ω から出発し、基本領域上の関数である楕円関数 $\wp(z)$ に対し、点 $(\wp(z),\ \wp'(z))$ の集合が楕円曲線 E をなすことを見てきた。この楕円曲線 E は格子 Ω によって定まるから、$E=E_\Omega$ と書いてもよい

今、楕円曲線全体の集合を考えるに際し、これとは逆側の論証が必要になる。すなわち、はじめに任意の楕円曲線 E から出発し、それに対して $E=E_\Omega$ となるような Ω が必ず存在するかという問題を考える必要がある。実は、これは「一意化定理(uniformization theorem)」と呼ばれる有名な事実であり、数論や代数幾何学の代表的なテキストにその証明を見ることができる。この定理によって、先ほど見た格子から楕円曲線を構成することができる。
したがって、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。
格子は

$$\Omega=\langle\omega_1\ ,\ \omega_2\rangle=\omega_2\left\langle\frac{\omega_1}{\omega_2},\ 1\right\rangle$$

と定数倍をくくりだせば、第二成分を 1 に揃えることができる。
一般に格子 Ω の複素数倍 $\lambda\Omega(\lambda\in\boldsymbol{C})$ は、λ が非零ならば、Ω に相似な格子（平面内の点列として相似な図形）となる。すなわち、適当な拡大・縮小と回転移動を施せば、互いにぴったり重ねあわせることができるのだ。そして、相似な格子に体しては、定義からすぐにわかるように、

$$g_2(\lambda\Omega)=\lambda^{-4}g_2(\Omega)$$
$$g_3(\lambda\Omega)=\lambda^{-6}g_3(\Omega)$$

が成立する。したがって、g_2^3 と g_3^2 は、ともに $\lambda\Omega$ を代入すると λ^{-12} がでてきて、λ の同時式となる。そして、先ほどの定理 3 で登場した判別式

$$\triangle(\Omega)=g_2(\Omega)^3-27g_3(\Omega)^2$$

もまた $\triangle(\lambda\Omega)=\lambda^{-12}\triangle(\Omega)$ を満たす。よって比

$$j(\Omega)=1728\ \frac{g_2(\Omega)^3}{\triangle(\Omega)}$$

を考えると、これは $\Omega\to\lambda\Omega$ の変換で変わらない。すなわち、

$$j(\lambda\Omega)=j(\Omega)$$

を満たす。この $j(\Omega)$ を *j*-不変量 *invaliant* と呼ぶ。
なお、係数 1728 がついているのは、フーリエ展開の初項の係数（無限遠点における留数）を 1 に揃えるためであり、本書の論議には関係ない。

j-不変量は格子の相似変換に関して不変であるから、上に見た格子の生成元の第二成分を１に揃えれば、第一成分だけで決まる。すなわち、格子を

$$\Omega = \langle \omega_1, \omega_2 \rangle = \omega_2 \left\langle \frac{\omega_1}{\omega_2}, 1 \right\rangle$$

と表し、ここで、$\tau = \dfrac{\omega_1}{\omega_2}$ とおけば、j-不変量は τ の関数とみなせるのだ。これを改めて $j(\tau)$と書こう。（今後は格子 Ωに体する $j(\Omega)$という記号は用いないことにする)。

元来の定義 $\tau = \dfrac{\omega_1}{\omega_2}$ によれば、τ は複素数全体を取り得ることになるが、元々、楕円曲線は格子によって決まるのだから、同じ格子 Ωに対応する τ が複数ある場合は、その中から１つだけ考えればよい。

まず、格子の第一成分 $\omega 1$ と第二成分の $\omega 2$ を入れ替えても格子は変わらないので、偏角の大きな方を第一成分にとることに決めておこう。すなわち、必要なら第一成分と第二成分を入れ替えて、いつも必ず $arg\ \omega 1 > arag\ \omega 2$ が成り立つ ものと仮定する。そうすると、$\tau = \dfrac{\omega_1}{\omega_2}$ は、上半面 Hの点となる。よって $j(\tau)$は、H 上の関数である。

さらに、定理１で見たように、H の中でもモジュラー群の作用で移り合う点どうしは同じ格子を表す。したがって、格子の全体に対して j の値を考えるためには、 τ をモジュラー群の基本領域の点の全体にわたらせればよい。

こうして、我々は、楕円曲線の全体からなる集合を格子の相似で分類し、各類から １ つずつ代表を選んだときにできる集合が、モジュラー群の基本領域と同じであることを見た。これを、楕円曲線の**モジュライ空間**と呼ぶ。

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−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。このとき、2 つの楕円曲線がモジュライ空間の点とみなすことができる。このとき、2 つの楕円曲線がモジュライ空間の中で同じ点になるかどうかは、$j(\tau)$の値によって判別できるというわけである。

本冊子のしめくくりに、先ほど定理 3 で登場した判別式

$$\triangle(\Omega)=g_2(\Omega)^3-27g_3(\Omega)^2$$

の意義について触れておこう。
これは格子 Ω から決まる値であるが、上で見たようにして上半面内の複素数 τ の関数として $\triangle(\tau)$ と表すこともできる。この複素数 $\triangle(\tau)$ は、ラマヌジャンの△関数と呼ばれる。

$$\triangle=x\prod_{n=1}^{\infty}(1-x^n)^{24}=\sum_{n=1}^{\infty}\tau(n)\,x^n$$

上式で、$x=e^{2\pi i}$ としたときの値が、$\triangle(\tau)$ になるのだ。

ラマヌジャン予想とは、係数
$\tau(n)$ $(\tau(1)=1,\ \tau(2)=-24,\ \tau(3)=252,\ \tau(4)=-1472\ \ .....)$
に関して、p が素数なら不等式

$$|\tau(p)|\ <\ 2p^{11/2}$$

が成り立つ。
この 11/2 という数値の意味については、別途解説する。

最後に佐藤テイト予想を記す。

佐藤テイト予想

$|\tau(p)|\ =\ 2p^{11/12}\cos\theta$ とおくと

$$\lim_{N\to\infty}\frac{(N\text{以下の素数}\alpha\leq\theta\leq\beta\text{を満たす者の個数こ})}{(N\text{以下の素数}p\text{の個数})}$$
$$=\frac{2}{\pi}\int_{\alpha}^{\beta}\sec^2\theta\,d\theta$$

が成り立つ。