Fermat's Enigma

$n$ を 3 以上の自然数とする．$(x,y,z)=(a,b,c)$ が方程式

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

の解ならば，$a,b,c$ の少なくとも 1 つは 0 である．

$n=lm$ と分解すると，$(x,y,z)=(a,b,c)$ が方程式 $x^n+y^n=z^n$ の解ならば，$(x,y,z)=(a^m,b^m,c^m)$ は方程式 $x^l+y^l=z^l$ の解である．3 以上の自然数 $n$ をわりきる 3 以上の自然数のうち最小のものは 3 以上の素数か 4 だから，$l=n$ が 3 以上の素数か 4 の場合に示せば，3 以上のすべての自然数 $n$ について示したことになる．

Fermat：$n=4$ のときに証明.

Euler: $n=3$ のときに証明.

多くの数学者による部分的な結果のあとに，Wiles が一般の $l$ について証明.

Wiles の方法：志村・谷山予想を証明することで，Fermat の最終定理を証明.

志村・谷山予想：有理数体上の楕円曲線はすべて保型形式と結びついている．

Wiles の部分的な結果のあと，Breuil-Conrad-Diamond-Taylor が一般の場合を証明. Fermat の最終定理の証明のためには，Wiles の結果で十分.

$n=3,4$ の場合と，$n=l\geq 5$ の場合の違い.

$n=3,4$ のとき：楕円曲線 $x^3+y^3=1$ と $y^2=x^3-x$ に座標が有理数の点がないことを証明.

$n=l\geq 5$ のとき：楕円曲線 $y^2=x(x-a^l)(x-c^l)$ そのものがないことを証明.

背理法による証明のながれ.

・方程式 $x^l+y^l=z^l$ の解 $(x,y,z)=(a,b,c)$ があったとする．

・楕円曲線 $y^2=x(x-a^l)(x-c^l)$ が，保型形式 $f=\sum_{n=1}^{\infty}a_nq^n$ と結びついていることを証明する.（Wiles）

・レベル 2 の保型形式 $g=\sum_{n=1}^{\infty}b_nq^n$ で，すべての $n\geq 1$ に対し $b_n-a_n$ が $l$ でわりきれるものが存在することを証明する.（Ribet）

・$a_1$ なのに，レベル 2 の保型形式は 0 だけなので矛盾が得られる．

楕円曲線 $y^2=x(x-a^l)(x-c^l)$ を考えるところが 1 つのポイント（Frey）

楕円曲線と保型形式，およびそれらの関係が重要.

講義の内容：

１．楕円曲線.

２．保型形式.

３．それらの関係.

# 1　楕円曲線

曲線：2 変数の多項式 $f(x,y)$ に対し，$f(x,y)=0$ で定義された図形.

$f(x,y)$ が 1 次式のとき：直線
2 次式のとき：2 次曲線．円，楕円，放物線，双曲線．
3 次式のとき：楕円曲線 $\neq$ 楕円
名前の由来：楕円積分．積分の計算

$$\int \frac{1}{\sqrt{x^2-1}}dx = ?$$

双曲線 $x^2-y^2=1$ を考え，$t=x+y$ とおけば，$\dfrac{1}{t}=x-y$ だから

$$x=\frac{1}{2}\left(t+\frac{1}{t}\right), y=\frac{1}{2}\left(t-\frac{1}{t}\right), \frac{dx}{dt}=\frac{1}{2}\left(1-\frac{1}{t^2}\right)$$

であり，

$$\int \frac{1}{\sqrt{x^2-1}}dx = \int \frac{1}{y}\frac{dx}{dt}dt = \int \frac{1}{t}dt = \log t = \log(x+\sqrt{1-x^2}).$$

積分が計算できる根拠：双曲線 $x^2-y^2=1$ の有理関数によるパラメータ表示

$$x=\frac{1}{2}\left(t+\frac{1}{t}\right), y=\frac{1}{2}\left(t-\frac{1}{t}\right)$$

$$\int \frac{1}{\sqrt{x^3-1}}dx$$

ではどうか．初等関数では積分を表わせない．楕円の弧長の計算にでてくるので，楕円積分とよばれる．楕円曲線 $y^2=x^3-1$ を，有理関数でパラメータ表示することはできない．

整数論的な問題意識．整数係数の多項式

$$y^2=x^3+ax+b$$

で定義される楕円曲線が重要．

たとえば，有理点についての Mordell の定理．Birch—Swinnerton-Dyer 予想など．100 万ドル懸賞問題．

Fermat が余白に書き込んだ本：Diophantus（古代ギリシャの数学者）．有理点を次々に構成．

$P$ での接線には，もう一つの交点 $Q$ がある．

複素数解はわかりやすい．$\omega_1,\omega_2$ を複素数で，$\omega_1/\omega_2=\tau$ が実数でないものとする．

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2}+\sum_{m,n\in\mathbb{Z};(m,n)\neq(0,0)}\left(\frac{1}{(z-(m\omega_1+n\omega_2))^2}-\frac{1}{(z-(m\omega_1+n\omega_2))^2}\right),\\
\wp'(z) &= -2\sum_{m,n\in\mathbb{Z}}\frac{1}{(z-(m\omega_1+n\omega_2))^3}
\end{aligned}$$

とおき，さらに，

$$g_2 = 60 \sum_{m,n\in\mathbb{Z};(m,n)\neq(0,0)} \frac{1}{(m\omega_1+n\omega_2)^2}, \quad g_3 = 140 \sum_{m,n\in\mathbb{Z};(m,n)\neq(0,0)} \frac{1}{(m\omega_1+n\omega_2)^3}$$

とおけば，$(x,y)=(\wp(z),\wp'(z))$ は方程式

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

をみたす．$\wp(z)$ や $\wp'(z)$ を楕円関数という．

Diophantus の方法：$P=(\wp(z),\wp'(z))$ なら $Q=(\wp(-2z),\wp'(-2z))$.

# 2　保型形式

$H=\{z\in\mathbb{C}|\mathrm{Im}\ z>0\}$ を上半平面という．

保型形式：$H$ 上定義された正則関数 $f(z)$ のうち，特別な性質をみたすもの．

性質１．$f(z+1)=f(z)$

$q=\exp(2\pi iz)$ とおくと，$f(z)=\sum_{n=-\infty}^{\infty}a_nq^n$ と表わせる．$z=x+iy$ のとき，

$$q=\exp(2\pi iz)=e^{-2\pi y}(\cos 2\pi x + i\sin 2\pi y)$$

だから，$y>0$ なら $|q|<1$. $q(z+1)=q(z)$.

性質２．$n<0$ なら（$n\leq 0$ なら）$a_n=0$.

$f(z)=\sum_{n=0}^{\infty}a_nq^n$. （カスプ形式）

性質３．整数 $a,b,c,d\in\mathbb{Z}$ で，$ad-bc=1$ かつ $c$ が $N$ でわりきれるものに対し，

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^{2k}f(z)$$

がなりたつ．

重さ $2k$，レベル $N$ の保型形式（カスプ形式）

$z$ を $\dfrac{az+b}{cz+d}$ にうつす変換は，上半平面での合同変換を表わしている．

上半平面 $H$：非ユークリッド幾何の舞台

ユークリッド幾何：ふつうの平面幾何．平行線公理がなりたつ．

平行線公理：直線 $l$ 外の一点 $P$ をとおり，$l$ と平行な直線はただ１つ存在する．

非ユークリッド幾何：平行線公理以外はユークリッド幾何と同じ条件をみたす幾何学．

例１．球面上の幾何：球の中心をとおる平面との共通部分である円を直線とよぶ．直線 $l$ 外の一点 $P$ をとおり，$l$ と平行な直線は１つも存在しない．

例２．上半平面上の幾何（双曲幾何）：実軸上に中心がある半円か，実軸と直交する半直線を直線とよぶ．直線 $l$ 外の一点 $P$ をとおり，$l$ と平行な直線はいくらでも存在する．

上半平面は単位円 $\{z\in\mathbb{C}||z|<1\}$ と同等．

# 3　楕円曲線と保型形式の関係

$L$ 関数

素数が無限個あることの Euler による証明

$1+\frac{1}{2}+\cdots+\frac{1}{n}>\log n\to\infty$ だから，$1+\frac{1}{2}+\cdots+\frac{1}{n}+\cdots=\infty$. 素因数分解の一意性より

$$\begin{aligned}&1+\frac{1}{2}+\cdots+\frac{1}{n}+\cdots\\ =\ &(1+\frac{1}{2}+\frac{1}{4}+\cdots)(1+\frac{1}{3}+\frac{1}{9}+\cdots)\cdots\\ =\ &\frac{1}{1-\frac{1}{2}}\frac{1}{1-\frac{1}{3}}\frac{1}{1-\frac{1}{5}}\cdots\end{aligned}$$

右辺が発散 $\Leftrightarrow \frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots$ が発散．よって，素数は無限個．$s>1$ なら

$$\zeta(s)=1+\frac{1}{2^s}+\cdots+\frac{1}{n^s}+\cdots=\frac{1}{1-\frac{1}{2^s}}\frac{1}{1-\frac{1}{3^s}}\frac{1}{1-\frac{1}{5^s}}\cdots$$

は収束.

$\zeta(s)$ を複素数変数の関数として定義し，素数の分布とむすびつけて研究（Riemann）.

$s=-2,-4,-6,\ldots$ なら $\zeta(s)=0$

Riemann 予想：それ以外の $\zeta(s)=0$ をみたす複素数 $s$ は，すべて Re $s=\frac{1}{2}$ がなりたつ．これも 100 万ドル懸賞問題.

ペレルマンがほかの 100 万ドル懸賞問題（Poincare 予想）を解決したが，100 万ドルもらわなかった.

いろいろなゼータ関数がある．楕円曲線の L 関数もその一種.

$y^2=x^3+ax+b$ で定義される楕円曲線を $E$ で表わす．各素数 $p$ に対し，整数 $a_p(E)$ を定義し，$L$ 関数を

$$L(E,s)=\prod_p\frac{1}{1-a_p(E)p^{-s}-p^{1-2s}}$$

で定義する.

$a_p(E)$ の定め方：

保型形式との結びつき：無限積を展開すると $L(E,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ と表わせる.

志村・谷山予想：$\sum_{n=1}a_nq^n$ が保型形式である.