数理解析研究所講究録 1219 巻 2001 年 1-10

不定方程式研究の現状の紹介

東北大学・理学研究科　森田 康夫
Yasuo Morita
Graduate School of Mathematics, Tohoku University

§0. 序

不定方程式を解くとは，整数係数の $x_1, x_2, \ldots, x_n$ の多項式 $F(x_1, x_2, \ldots, x_n) \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$ から定まる次の方程式 (♯) の整数解を求めることを言う：

$$(\sharp) \quad F(x_1, x_2, \ldots, x_n) = 0 \qquad (x_1, x_2, \ldots, x_n \in \mathbf{Z})$$

不定方程式に関する基本的な問題は，(1) 不定方程式 (♯) は解を持つかどうかを判定し，(2) (♯) が解を持つなら，どの程度多く解を持つかを調べ，さらに (3) (♯) のすべての解を求めることである．しかし，一般的にはいずれも不可能であり (§3 参照)，これらの問題が解ける場合を見つけることが課題となる．

この問題を幾何学的に解釈すると次のようになる：

$$V(\mathbf{C}) = \{(x_1, x_2, \ldots, x_n) \in \mathbf{C}^n \mid F(x_1, x_2, \ldots, x_n) = 0\}$$

と置くと，n 次元空間 $\mathbf{C}^n$ の中の代数多様体ができる．(♯) が整数解を持つかどうかという問題は，この代数多様体の上に座標が整数の点 (**整数点**) が有るかどうかという問題になる．同様にこの方程式 (♯) の有理数解を求める問題は，この代数多様体の上に座標が有理数の点 (**有理点**) が有るかどうかという問題になる．こちらの方が，やや易しくなる[1]．

いずれにしろ，これらの問題には多様体 V の幾何学が深く関係している．その意味でこれらの問題は，数論的幾何学の代表的問題として，多くの人により研究されている．

歴史的には，有理数解を求める問題は **Diophantus**(246?–330?) が研究し，整数解を求める問題は **P. de Fermat**(1601–1665) が研究を始めた．そのため不定方程式を解く問題を，**Diophantus 問題**とも言う．

不定方程式の例としては，Fermat の方程式 $x^n + y^n = z^n$ $(n \geq 3)$ が有名だが，数学の世界では不定方程式は頻繁に出て来る．例えば二次体の整数論は，二元二次の不定方程式 $x^2 - dy^2 = m$ $(d, m \in \mathbf{Z})$ の研究から生まれた．整数論はもちろん，代数多様体，群，表現論などの研究を行っているとき，問題が不定方程式に帰着する場合が頻繁に有り，そこに不定方程式の研究の重要性の 1 つが有る．

[1] 整数解に関する問題の方が，よりデリケートという意味．Fermat はこの 2 つの問題のデリケートの差を強調している．

§1. 局所体への埋め込みと，方程式の特殊な形の利用

有理数体 $\mathbf{Q}$ は実数体 $\mathbf{R}$ の部分体だから，平方数の形に書ける元は正であり，例えば不定方程式 $1+2x^2+3y^4+5z^6=0$ は有理数解を持たない．

これは有理数体の実数体への埋め込み $\mathbf{Q}\hookrightarrow\mathbf{R}$ を使い，実数体 $\mathbf{R}$ の性質を使って不定方程式の性質を導いたものだが，同様にして p-進体への埋め込み $\mathbf{Q}\hookrightarrow\mathbf{Q}_p$ を使って不定方程式の性質を導くこともできる．

例えば不定方程式 $x^2+3y^4=10$ は，整数の 2 乗 n^2 は modulo 4 では 0 または 1 となるから，左辺は modulo 4 では 0 , 1 , 3 となり，他方右辺は modulo 4 では 2 だから，整数解を持たない．これは 2-進体への埋め込み $\mathbf{Q}\hookrightarrow\mathbf{Q}_2$ を使ったものである．

もう少し非自明な例を述べるため，

$$f(x,y)=a_0x^n+a_1x^{n-1}y+\cdots+a_{n-1}xy^{n-1}+a_ny^n \qquad (a_0,a_1,\ldots,a_n\in\mathbf{Z})$$

を重根を持たない $n\geq 3$ 次の規約な同次多項式とする．このとき不定方程式

$$f(x,y)=m \qquad (m\in\mathbf{Z})$$

を Thue の方程式と呼ぶ．

この方程式の左辺は，

$$a_0\,y^n\prod_{i=1}^{n}\left(\frac{x}{y}-\alpha_i\right)=m \qquad (\alpha_i\text{は}f(x,1)=0\text{の解となる代数的数})$$

と書けるから，結局，代数的数 α_i が有理数 x/y でどの程度近似できるかが問題となる．そこでこの近似 (Diophantus 近似) の問題を研究することにより，次の定理が証明される ([7] 参照)：

定理. Thue の方程式は，有限個しか整数解を持たない．

この定理以外にも，方程式の特殊な形を利用することにより，解の性質が分かる場合が色々ある．しかし我々の目から見て面白いのは，以下の様な不定方程式についての一般的な理解が得られる場合である．

§2. 低次の不定方程式

一番やさしい不定方程式は，1 次の不定方程式

$$ax=b \qquad (a,b\in\mathbf{Z})$$

である．明らかに，この方程式は b が a の倍数のときに限り解を持ち，$x=(b/a)m$ $(m\in\mathbf{Z})$ がその解となる．

これを一般化した n 変数の m 個の連立 1 次不定方程式

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

$(a_{ij}, b_i \in \mathbf{Z},\ x_i \in \mathbf{Z})$ は，行列の単因子の理論を使うと

$$c_1y_1 = d_1,\ c_2y_2 = d_2,\ \ldots\ldots\ldots,\ c_my_m = d_m \qquad (c_i, d_i \in \mathbf{Z})$$

の形の不定方程式に帰着され，1 変数の場合の結果を使うと容易に解ける．

二元二次の不定方程式 $x^2 - dy^2 = m$ $(d, m \in \mathbf{Z})$ については，この方程式を

$$(x - y\sqrt{d})(x + y\sqrt{d}) = m$$

と因数分解し，$\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{d}$ という環で m の 2 つの数 $(x - y\sqrt{d})$, $(x + \sqrt{d})$ への分解を考えることになる．この方針で二元二次の不定方程式は，(2 次体の整数論を使って) 解くことができる (高木貞治 [11] 参照)．より正確に言うと，2 次体の整数論や代数体の整数論は，こういった研究から生まれた．

一般に $x_1, x_2, \ldots, x_n$ の整数係数の 2 次式を $F(x_1, x_2, \cdots, x_n)$ とするとき，不定方程式 $F(x_1, x_2, \cdots, x_n) = 0$ の解を求める方法を，C. L. Siegel(1896–1981) は発見した．しかし，一般の連立の 2 次の不定方程式を解く方法が存在しないことは，Hilbert の第 10 問題との関連で分かっている (§3 参照)．

§3. Hilbert の第 10 問題

D. Hilbert(1862–1943) は，1900 年にパリで開かれた国際数学者会議で，20 世紀のうちに解かれるべき 23 の数学の問題を提出したが，そのうちの第 10 問題として，「任意の与えられた不定方程式が整数解を持つかどうかを，有限回で判定するアルゴリズムを求める」問題を提出した．§3 では，この問題を考察する．

まず連立の不定方程式

$$F_1(x_1, x_2, \ldots, x_n) = 0, \ldots\ldots\ldots\ldots, F_m(x_1, x_2, \ldots . x_n) = 0$$

を解くことは，

$$F_1(x_1, x_2, \ldots . x_n)^2 + \ldots\ldots\ldots + F_m(x_1, x_2, \ldots . x_n)^2 = 0$$

を解くことと同値である．したがって，単独の不定方程式を研究すれば十分である．

さて，任意の多項式は和と差と積から作れる．とくに新しい変数 $z = x \times y$ を導入することにより，2 次式 $x \times y$ を 1 次式 z で置き換え，次数を下げることができる．こ

のことから，任意の不定方程式は高々2次の連立の不定方程式に帰着できることが分かる．したがって，任意の2次の連立不定方程式を解くことは，任意の不定方程式を解くことと同じ難しさを持つ．

任意の整数 x は正の整数の差 $x = y - z$ $(y, z \in \mathrm{N})$ と書けるから，不定方程式 $F(x_1, x_2, \ldots, x_n) = 0$ が整数解を持つかどうかを調べるには，不定方程式 $F(y_1 - z_1, y_2 - z_2, \ldots, y_n - z_n) = 0$ が正の整数解 $y_1, z_1, \ldots, y_n, z_n \in \mathrm{N}$ を持つかどうかが判定できれば十分である．

逆に任意の非負の整数 x は，J. L. Lagrange(1736–1813) の定理により，4個の整数の2乗の和 $x_{(1)}^2 + x_{(2)}^2 + x_{(3)}^2 + x_{(4)}^2$ の形に書けるから，不定方程式 $F(x_1, x_2, \ldots, x_n) = 0$ が正の整数解を持つかどうかを調べるには，不定方程式

$$F(1 + x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2, 1 + x_{21}^2 + x_{22}^2 + x_{23}^2 + x_{24}^2, \ldots, 1 + x_{n1}^2 + x_{n2}^2 + x_{n3}^2 + x_{n4}^2) = 0$$

が整数解 $x_{11}, x_{12}, x_{13}, x_{14}, \ldots, x_{n1}, x_{n2}, x_{n3}, x_{n4} \in \mathrm{Z}$ を持つかどうかが判定できれば十分である．したがって，Hilbert の第10問題を研究するには，「任意の不定方程式が正の整数解を持つかどうかを判定するアルゴリズム」の存在を研究すれば十分である．

自然数の組の上で定義された自然数に値を取る関数 $f : \mathrm{N}^n \longrightarrow \mathrm{N}$ について，**再帰関数** (recursive function) という概念が有る．これは，(i) 定数関数 $f(x_1, x_2, \ldots, x_n) = c$ $(c \in \mathrm{N})$，(ii) ある変数 x_i を取り出す関数 $f(x_1, x_2, \ldots, x_n) = x_i$，(iii) 1をたす関数 $f(x) = x + 1$ から数学的帰納法などを使って定義される関数の全体を言う．これは，値が有限回の手続きで計算できる関数の全体と一致するものと考えられている．

他方 N^n の部分集合 S は，適当な多項式 $P(y_1, \ldots, y_m, x_1, \ldots, x_n)$ が有り，

$$S = \{(x_1, \ldots, x_n) \in \mathrm{N}^n \mid P(y_1, \ldots, y_m, x_1, \ldots, x_n) = 0 \text{ は解 } y_1, \ldots, y_m \in \mathrm{N} \text{ を持つ}\}$$

と書けるとき，**不定方程式型**であると言う．また，自然数の組の上で定義された自然数に値を取る関数 $f : \mathrm{N}^n \longrightarrow \mathrm{N}$ については，そのグラフ $\mathrm{graph}(f) \subset \mathrm{N}^{n+1}$ が不定方程式型のとき，**不定方程式型**であると言う．

不定方程式型の関数が再帰関数であることはすぐ分かるが，**Y. Matiyasevič** 等の基礎論のグループの人達は，次のことを証明した (1970, M. Davis [4] 参照)：

定理． 関数 $f : \mathrm{N}^n \longrightarrow \mathrm{N}$ は，不定方程式型になるとき，そのときに限り，再帰的になる．

これ以前より基礎論では，自然数の再帰的部分集合 $S \subset \mathrm{N}$ で，その補集合 $S^c = \{n \in \mathrm{N} \mid n \notin S\}$ が再帰的でないものが存在することが知られていた．そこで定理を使い，この S を多項式 $P(y_1, y_2, \ldots, y_m, x)$ を使って

$$S = \{x \in \mathrm{N} \mid P(y_1, y_2, \ldots, y_m, x) = 0 \text{ は解 } y_1, y_2, \ldots, y_m \in \mathrm{N}^m \text{を持つ}\}$$

と不定方程式型に表現すると，「パラメーター x を含む $y_1, y_2, \ldots, y_m$ についての不定方程式

$$P(y_1, y_2, \ldots, y_m, x) = 0 \qquad (x \in \mathrm{N})$$

が，どの x に対して自然数解を持つか？」を判定するアルゴリズムは存在しないことが分かる．これより，Hilbert の第 10 問題は解が存在しないことが分かる．

Hilbert の第 10 問題に関連した未解決な問題としては，

(1) 任意の不定方程式が有理数解を持つかどうかを判定するアルゴリズムが存在するか?

(2) 不定方程式の解が取る範囲を整数環 $\mathbf{Z}$ から有限次代数体 K の整数環 $\mathcal{O}_K$ にした場合に，$\mathcal{O}_K$ 係数の不定方程式が $\mathcal{O}_K$ の中に解を持つかどうかを判定するアルゴリズムが存在するか？

などが有る．いずれもかなり難しい問題のようである．

§4. Birch + Swinnerton-Dyer 予想と Mordell 予想

序文でも述べたように不定方程式

$$F(x_1, x_2, \ldots, x_n) = 0 \qquad (x_1, x_2, \ldots, x_n \in \mathbf{Q})$$

を解く場合には，対応する代数多様体

$$V = V(\mathbf{C}) = \{(x_1, x_2, \ldots, x_n) \in \mathbf{C}^n \mid F(x_1, x_2, \ldots, x_n) = 0\}$$

の幾何学が密接に関係している．§4 では，この代数多様体が 1 次元の代数曲線となる場合を調べる[2].

代数曲線には，**種数**と呼ばれる不変量 $g \in \{0, 1, 2, \ldots\}$ が有る．

種数が 0 の代数曲線が関係する不定方程式の例としては，2 変数の 2 次式 $y^2 = ax^2 + bx + c$ $(a, b, c \in \mathbf{Q})$ が有る．このような種数が 0 の代数曲線については，整数点も有理数点も有限回の計算ですべて求めることができる．

次に種数が $g = 1$ となる場合を考える．この場合に限っても，整数解や有理数解が存在するかどうかを判定するアルゴリズムはまだ未発見だが，とりあえず，V には少なくとも 1 つ有理数解が存在するものとする．このとき，適当な有理数を係数とする変数変換をすると，問題の不定方程式は

$$y^2 = x^3 + ax^2 + bx + c \qquad (a, b, c \in \mathbf{Q})$$

の形に書ける．このようなものを，有理数体 $\mathbf{Q}$ 上定義された**楕円曲線** (elliptic curve) と呼ぶ．

---

[2]以下有理点を考える場合には，完備化と特異点の還元を行い，完備非特異な代数曲線を考える．元の曲線の上の有理点と，完備化し特異点の還元を行った代数曲線の上の有理点は，有限個の例外点を除き一対一に対応する．

V が楕円曲線なら，V の有理点の全体 $V(\mathbf{Q})$ は有限生成のアーベル群となることが分かっている (Mordell , 1922). そこでその構造が問題になるが,「アーベル群 $V(\mathbf{Q})$ の階数は，V からある方法で定義されるゼータ関数[3] $Z(s;V)$ の $s=1$ での零点の位数に等しいだろう」と予想されている (**Birch + Swinnerton-Dyer 予想**). さらに $V(\mathbf{Q})$ の生成元が作る行列 (regulator) が，$Z(s;V)$ の $s=1$ での展開を使って書けるだろうとの予想されており，その系として，$V(\mathbf{Q})$ の生成元が計算可能だと予想されている. これらの予想は，現在でもまだ完全には解けていず，数論的幾何学における最も重要な未解決の問題の一つである.

次に，V の種数が 2 以上の場合を考える. この場合に **L. J. Mordell**(1888–1972) は,「V の座標が有理数の点の全体は有限集合になるだろう」と予想した (**Mordell 予想**). Mordell 予想は，予想が作られてから 50 年もの間解けなかったが，1983 年 **G. Faltings** は他の重要な予想[4]と共に Mordell 予想を証明した. さらにこの場合には，V の有理点を有限回の操作で求めるアルゴリズムが存在するものと思われている (**Effective Mordell Conjecture**).

なおこの節では簡単のため有理数体 $\mathbf{Q}$ 上で説明したが，有限次代数体 K をとっても同様になる.

§5. Gelfond と Baker の仕事

A. O. Gelfond(1906–68) は,「α, β が 0 でない代数的数なら，その比 $\log(\beta)/\log(\alpha)$ は，有理数でなければ超越数となる」ことが成立つことを示した[5]. さらに彼は

α, β が 0 でない代数的数で，その比 $\log(\beta)/\log(\alpha)$ が有理数でないとき，0 でない有理数 a, b を係数に持つ一次形式 $a\log(\alpha)+b\log(\beta)$ がどれだけ 0 に近づけるか？

という問題を研究し，この問題の解答が整数論の色々な問題に応用できることを示した. Gelfond はこの問題を一般の代数的数の一次結合に拡張することを提案したが，Gelfond のアイデアは，**A. Baker**(1939–) により実現された (A. Baker [1] 参照) :

これにより，Baker は Gelfond のプログラムを実行することができ，不定方程式の解の研究や小さな類数を持つ虚二次体の決定に使用した. Baker は不定方程式への応用として，例えば次のことを示した :

定理. K を有限次代数体，$\alpha_1, \ldots, \alpha_n$ を K の代数的整数とする. このとき，不定

---

[3] Hasse-Weil のゼータ関数. 素数 p で V の方程式の $\bmod p$ を取ってできる方程式の有限体 $\mathbf{F}_{p^m}$ $(m \geq 1)$ における解の個数を使って定義する.

[4] アーベル多様体に関する Tate 予想など.

[5] このことは，a, b が代数的数で，$a \neq 0, 1$ かつ b が有理数でないなら a^b は超越数であること (Gelfond と T. Schneider の定理) を意味する. これより Hilbert の第 7 問題にで例示された数 $2^{\sqrt{2}}$ の超越性が分

$$Y^2 = (X-\alpha_1)\cdots(X-\alpha_n)$$

の X, Y が K の代数的整数となる解をすべて求めることができる[6].

さて Baker の定理は，D. W. Masser と G. Wüstholz により，対数関数 $\log : \mathbf{C}^\times \longrightarrow \mathbf{C}$ を，可換な線形代数群 G からそのリー環 $\mathcal{G}$ への対数写像で置き換える一般化が行われた．また Masser - Wüstholz の定理の不定方程式への応用も研究されている[7]．さらに彼らの結果を使って，「種数が 2 以上の代数曲線の上の有理点を有限回の操作で求めること」(effective Mordell 予想) が可能になろうとしている．

このことと，Masser と Wüstholz の評価を改良し，その応用を追求することがこの分野の残された重要な問題であるが，これについての解説は平田典子に譲る．

§6. 有理点の漸近分布

この節の結果も，基礎体 K が有理数体 $\mathbf{Q}$ でないときにも拡張できるが，簡単のため[8]有理数体 $\mathbf{Q}$ の場合に限り説明する．

射影空間 $\mathbf{P}^n$ などの上には有理点 (座標が有理数の点) は無限個存在するから，なにか尺度をつけたほうが便利である．そこで以下のようにして高さを定義する：

$P = [x_0; x_1; \ldots; x_n]\,(x_0, x_1, \ldots, x_n \in \mathbf{Q})$ を射影空間 $\mathbf{P}^n$ の点の同次座標とする．ここで同次座標は，すべての座標に同じ数をかけても同じ点をあらわすことに注意し，$x_0, x_1, \ldots, x_n$ の分母を払い，共通な因数で割り，$x_0, x_1, \ldots, x_n$ を最大公約数が 1 の整数の組にする．P をこのような $x_0, x_1, \ldots, x_n$ を使って表すとき，

$$H(P) = \max\{|x_0|, |x_1|, \ldots, |x_n|\}$$

とおき，P の**高さ** (height) と呼ぶ．ここで $|\ |$ は絶対値を表すものとする．

このとき，任意の正の数 H に対して，$H(P) \leq H$ となる有理数を座標に持つ点 P の全体は有限集合になる．

$F_i(x_0, x_1, \ldots, x_n) \in \mathbf{Q}[x_0, x_1, \ldots, x_n]\ (i = 1, \ldots, m)$ を有理数を係数として持つ $x_0, x_1, \ldots, x_n$ の同次多項式とし，これらの共通零点の全体を

$$V = V(\mathbf{C}) = \{\,[x_1; x_2; \ldots; x_n] \in \mathbf{P}^n(\mathbf{C}) \mid F_i(x_0, x_2, \ldots, x_n) = 0\,(i = 1, \ldots, m)\,\}$$

とおく．また

$$V(\mathbf{Q}) = \{\,[x_1; x_2; \ldots; x_n] \in \mathbf{P}^n(\mathbf{Q}) \mid F_i(x_0, x_2, \ldots, x_n) = 0\,(i = 1, \ldots, m)\,\}$$

---

[6]有限回の計算ですべての解が求められると言う意味．どれだけ大変な有限回かは問わない．

[7]例えば志賀弘典は，この定理を使って Siegel modular 関数の値の研究をした．

[8]一般の場合は付値の一般論，とくに積公式が必要になる．

とおき，V の**有理点の集合**と呼ぶ．このとき，有理点の集合 $V(\mathbf{Q})$ のゼータ関数を次式で定める：

$$Z(V;s) = \sum_{P\in V(\mathbf{Q})} H(P)^{-s}$$

例．$n=1$ とすると，$P^1(\mathbf{C}) = \mathbf{C}\cup\{\infty\}$ となる．そこで $P = a/b \in \mathbf{Q}$ ($a\in\mathbf{Z}$, $b\in\mathbf{N}$, a,b は互いに素) を射影空間 $\mathbf{P}^1(\mathbf{Q})$ の点と見ると，$H(P) = \max(|a|,b)$ となる．よって $H(P)\le H$ なら $|a|,b\le H$ となり，このような点 P は有限個となる．

またこの場合のゼータ関数は，上の計算より，

$$Z(\mathbf{P}^1;s) = 2 + 2\sum_{H=1}^{\infty} \frac{\varphi(H)}{H^s}$$

となる．ただしここで $\varphi(H)$ は，Euler 関数 ($1\le m\le H$, $(m,H)=1$ となる自然数 m の個数) とする．

一般の射影空間 $\mathbf{P}^n$ の上の有理点 $P\in\mathbf{P}^n(\mathbf{Q})$ で $H(P)\le H$ をみたすものの個数 $N(H)$ の漸近分布は，S. H. Scanuel により求められた：

定理 $\mathbf{P}^n(\mathbf{Q})$ の点 P で，$H(P)\le H$ となるものの個数 $N(H)$ は，

$$N(H) = \zeta(n+1)^{-1}2^n(n+1)H^{n+1} + \mathrm{O}(H^n) \qquad (H\longrightarrow\infty)$$

で与えられる．ただし，$\zeta(n+1)$ は Riemann のゼータ関数 $\zeta(s) = \sum_{1\le n<\infty} n^{-s}$ の $s=n+1$ での値とし，$n=1$ のときは，誤差項 $\mathrm{O}(H^n)$ を $\mathrm{O}(H\log(H))$ で置き換える．

これより $\mathbf{P}^n(\mathbf{Q})$ のゼータ関数は，$\mathrm{Re}(s) > n+1$ のとき収束することが分かる．また，$V(\mathbf{Q})$ は $\mathbf{P}^n(\mathbf{Q})$ の部分集合だから，ゼータ関数 $Z(V;s)$ も $\mathrm{Re}(s)$ が十分大きいとき収束する．

V. V. Batyrev と **Yu. I. Manin** は V の標準束 (canonical bundle) を使って幾何学的不変量 $\alpha(V)$ を定義し，任意の正の数 ε に対し，$V(\mathbf{Q})$ から適当な多項式の零点集合 $F_\varepsilon\subset V(\mathbf{Q})$ を除いた集合 $U = U_\varepsilon = V\setminus F_\varepsilon$ を作ると，U_ε のゼータ関数

$$Z(U_\varepsilon;s) = \sum_{P\in U_\varepsilon(\mathbf{Q})} H(P)^{-s}$$

は，$\mathrm{Re}(s)$ が $\alpha(V)+\varepsilon$ より大きいとき収束すると予想した (V. V. Batyrev - Yu. I. Manin [2] 参照)．

ここで $\beta(U)$ を $Z(U;s)$ が $\mathrm{Re}(s) > \beta(U)$ のとき収束する最小の正の数とするとき，任意の $\varepsilon>0$ に対し

$$\{P\in U(\mathbf{Q}) \mid H(P)\le H\} \text{の元の数} = O(H^{\beta(U)+\varepsilon}) \qquad (H\to\infty)$$

という漸近表示が成り立つ．この意味で，$\beta(U)$ は U 上の有理点分布を表す．

$\beta(U)$ を使うと，上の予想は任意の $\varepsilon>0$ に対し，適当な (V の Zariski 位相での開集合) $U = U_\varepsilon$ を取ると $\beta(U) < \alpha(V)+\varepsilon$ となると言える．

V が種数が 2 以上の代数曲線なら $\alpha(V)$ が負になるから，Batyrev と Manin の予想は，$V(\mathbf{Q})$ から有限個の点を除いた集合 U_ε のゼータ関数が $\mathrm{Re}(s)$ が負のとき収束し，U_ε が有限集合となることを意味する．したがって，この予想から Mordell 予想 (Faltings の定理) が導かれる．

さらに，V が一般型の代数多様体なら $\alpha(V)$ が負になることから，この予想から Mordell 予想の一般化が得られる．また Batyrev - Manin の予想は，射影空間の場合の Shanuel の結果を一般化したものとなっており，V が 1 次元の時には，Faltings の定理を使って証明できる．さらに V がアーベル多様体のときにも，A. Néron の height の理論から導ける．

この予想の証明と精密化[9]も，現在残っている重要な問題である．

§7. Fermat の予想の解決とこれからの研究課題

一般の場合の **Fermat の最終定理**は，p を奇素数とするとき，不定方程式

$$(F_p) \qquad X^p + Y^p + Z^p = 0 \qquad (X, Y, Z \in \mathbf{Z})$$

が自明な解 ($XZY = 0$ となること) しか持たないことに帰着する．さらに a, b, c がこの不定方程式 (F_p) の自明でない解なら，楕円曲線 $y^2 = x\,(x - a^p)\,(x + b^p)$ がモジュラー関数から作れることになり，そのことから矛盾が導かれた (A. Wiles [12] 参照)．

この証明の本質的な部分として，$\mathbf{Q}$ 上定義される楕円曲線は，モジュラー関数から作ることができるという谷山豊・志村五郎・A. Weil による予想が有る．この予想を一般化して証明することも，現在の数学の重要な課題である．アーベル多様体に拡張することはできそうだが，例えば K3 曲面の場合にはどうなるのだろうか？

不定方程式の可解性に戻ると，Hilbert の第 10 問題の否定的解決により，一般に整数解が存在するかどうかを判定するアルゴリズムは存在しないことが分かり，それより有理数解が存在するかどうかを判定するアルゴリズムも存在しないものと思われている．それではどのような場合に限れば，これらのことは可能になるのだろうか？またすべての整数点や有理点を求めるアルゴリズムは，どのような場合に存在し，どのような場合には存在しないのだろうか？この問題の研究は，数学における最も重要な問題の 1 つだと思われる．

これらの問題は，1 次元の代数曲線に限れば解決可能に思われているが，2 次元の代数曲面の場合には，整数解ないしは有理数解の存在を判定できない例が有ると思われている．これらのことを確かめることは，非常に重要である．

また現在までの反例は，数学基礎論的な意味は明確だが，数論幾何学的な意味は不明確である．数論幾何学的に分かりやすい反例の構成も重要である．例えば，2 次元の一般型の代数曲面で反例が作れるのだろうか？2 次元の他の型ではどうなるのだろうか？

---

[9] 例えば，V が一般型の場合，$\beta(U)$ が負となる U が具体的に計算可能か，またその場合に U 上に有理点を具体的に研鑽することが可能か，などの研究である．

$\pi : S \longrightarrow C$ を代数曲線 C 上の楕円曲面とし，C, S, π などの定義方程式は $\mathbf{Q}$ 上定義されているとする．このとき定義より，π の一般のファイバー $E_t = \pi^{-1}(t)\,(t \in C)$ は楕円曲線となる．そこでさらに t が C の生成点であるとし，P_t を E_t の $\mathbf{Q}(t)$[10]-有理点であるとする．このとき，任意の C の点 c に対し P_t の座標に出てくる t に c を代入すると，$E_c = \pi^{-1}(c)$ の $\mathbf{Q}(c)$-有理点 P_c ができ，これらの点の全体 $\{P_c \mid c \in C\}$ は $\pi : S \longrightarrow C$ の切断を与える．とくに c が C の有理点なら，P_c は $E_c \subset S$ の有理点を与える．この意味で楕円曲面があると，切断から有理点が沢山作れるが，それ以外の有理点の性質を統一的に調べることは，非常に困難である．

同様のことは $K3$ 曲面 S でも生じ，S 上には多くの種数が 0 または 1 の代数曲線が有り，その上の有理点の性質は良く分かるが，それ以外の有理点の性質を調べることは非常に困難である．

どちらの場合も，これらの代数曲線上に乗らない有理点の性質を調べることは，どの程度まで可能だろうか？このような有理点をすべて求めることは可能だろうか？また不可能だとすると，Batyrev と Manin による評価以上の漸近的な性質を求めることは可能だろうか？現時点では，これらのことは殆ど分かっていない．

参考文献

[1] A. Baker, Transcendental number theory, Cambridge Univ. Press, 1975.

[2] V. V. Batyrev, Yu. I. Manin, Sur le nombre des points rationnels de hauteur borné des variétés algébriques, Math. Ann. **286**(1990), 27-43.

[3] M. Davis, Y. Matijasevič, and J. Robinson, Diophantine equations: Positive aspects of a negative solution, Proc. of Symposia in Pure Math., 28(1976), 233-269.

[4] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Monthly, **80**(1973), 233-269.

[5] G. Faltings, Entlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. math., **73**(1983), 349–366.

[6] D. Hilbert 著，一松信訳・解説，数学の問題，共立出版，1969.

[7] L. J. Mordell, Diophantine Equations, Academic Press, 1969

[8] 森田康夫，不定方程式を解く，数学のたのしみ，**17**(2000)，21-31.

[9] Yasuo Morita, Atsushi SATO, Distribution of rational points on hyperelliptic surfaces, Tohoku Math. J., **44**(1992), 345-358.

[10] Yasuo Morita, Remarks on a conjecture of Batyrev-Manin, Tohoku Math. J., **49** (1997), 437–448.

[11] 高木貞治，初等整数論講義，共立出版，1931.

[12] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math., **141** (1995), 443–551.

[10] $\mathbf{Q}$ 係数の t の座標の有理関数の全体を $\mathbf{Q}(t)$ で表す．