Ｔｈｕｅ の定理

成蹊大学理工学部　若　林　　功 (Isao Wakabayashi)

ここでは Thue の定理の紹介とその証明を与える．

$F(x,y)$ を既約な整数係数 d 次斉次多項式とする．$d\geqq 3$ とする．k を任意の整数とする．このとき，不定方程式

$$F(x,y)=k \quad x,y\in\mathbf{Z}$$

を Thue 方程式という．解を整数の範囲で求めることが問題である．以下，整数とは有理整数を表し，代数的整数には代数的を付ける．

一つ例を挙げる．

例　Thue 方程式 $2x^3-y^3=1$. この方程式については $(x,y)=(1,1),(0,-1)$ は解であることは直ちにわかる．しかしこれで全部か，というのは難しい問題で，初等的にはわからない．

不定方程式の歴史は古い．数学の起源と同じ程ともいえる．各辺の長さが自然数 (x,y,z) である直角三角形を求めることは，不定方程式 $x^2+y^2=z^2$ を解くことに相当する．良く知られた解に $(x,y,z)=(3,4,5),(5,12,13)$ があるが，古バビロニア期 (BC1900 ~ BC1600) の粘土板に自然数の三つ組み $(12709,13500,18541)$ が刻まれている．これが解であることは容易に確認できるが，これを見つけることは闇雲にはできないことで，この時代にこの地に高度な数学と文明があったことの証と見なせる．

Axel Thue(1863–1922) はノルウェーの数学者である．Thue 以前，19 世紀までは不定方程式はもっぱら代数的に研究された．扱われた対象も個別的であった．Thue は，本来代数的な問題である不定方程式を調べるのに解析を持ち込んだ．これは大きな視点の転換であった．得られた結果も一般的であった．

定理 (Thue, 1909)　α を 次数 $d\geqq 2$ の代数的数とする．$\varepsilon>0$ とする．

⇒

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^{\frac{d}{2}+1+\varepsilon}} \tag{1}$$

なる有理数解は有限個．

別の表現をするとこれは，有限個の (p,q) を除いて，

$$\left|\alpha-\frac{p}{q}\right|\geqq\frac{1}{|q|^{\frac{d}{2}+1+\varepsilon}}$$

が成り立つことを示している．すなわち，「代数的数は有理数であまり良く近似できない」ことを示している．

この定理は ineffective である．証明の仕方が，$C_1=C_1(\alpha,\varepsilon),\ C_2=C_2(\alpha,\varepsilon)$ があって，$q_1>C_1$ なる (1) の解があったとすると，その解をもとにして決まる定数より大きい (1) の解，すなわち $q_2>q_1^{C_2}$ なる解があったら矛盾，ということであるから．大きさの分からない解 q_1 を基にして，それ以外の解の上界が与えられるだけであるから．

この定理は Thue 方程式の解の有限性を与える．

定理′　Thue 方程式の解は有限個である．

上記定理が ineffective であることから，この定理′も ineffective である．すなわち，解の大きさの上界を与えることができない．解の上界は Baker の定理 (1968) によって初めて与えられた．Thue 方程式が特別な良い形をしている場合には，Padé 近似の方法によっても解の上界を与えることができる．この方法の起源も Thue にある．この場合にはかなり小さな上界を得ることができる．

なお，F が既約であるとした条件は緩められて，$F(x,1)=0$ が少なくとも三つの相異なる解をもてば定理′は成り立つ．

定理′の証明　F を因数分解し，$F(x,y)=a(x-\alpha y)(x-\alpha' y)\cdots(x-\alpha^{(d)}y)$ とする．(x,y) を解とし，$y\neq 0$ で，x/y が α に近いとすると，容易に

$$|x/y-\alpha|=\frac{|k|}{|a(x/y-\alpha')\cdots(x/y-\alpha^{(d)})||y|^d}<\frac{c}{|y|^d}$$

を得る．一方 Thue の定理から，有限個の (x,y) の組を除いて，

$$\left|\alpha-\frac{x}{y}\right|\geqq\frac{1}{|y|^{\frac{d}{2}+1+\varepsilon}}$$

となる．この二つから，

$$\frac{1}{|y|^{\frac{d}{2}+1+\varepsilon}}<\frac{c}{|y|^d}$$

となるが，$d\geqq 3$ のとき $d/2+1<d$ であるから，これから y の有限性を得る．

Thue の定理の証明の方針　証明には Siegel の補題，Wronski 行列式，Taylor 展開が用いられる．(1) を満たす有理数 p/q が無限個あると仮定する．代数点 α で多くの零をもつ多項式 $F(x)\in\mathbf{Z}[x]$ を作る．F は α で多くの零をもつので，α に非常に近い有理点 p/q での値 $F(p/q)$ は極めて小さくなる．一方有理点 p/q での F の値は $1/q^{\deg F}$ より小さくはなれない．これより矛盾を得ることを目指す．実際には F は整数係数ではうまくいかず，$F(x)=P(x)-\alpha Q(x),\ P,Q\in\mathbf{Z}[x]$ なる形のもので α で多くの零をもつものを作り，$F(p/q)$ の代わりに値 $\gamma=P(p_1/q_1)-(p_2/q_2)Q(p_1/q_1)$ を考える．γ は有理数であるから一方では小さくなれず，他方

$$\gamma=\left(P\left(\frac{p_1}{q_1}\right)-\alpha Q\left(\frac{p_1}{q_1}\right)\right)+\left(\alpha-\frac{p_2}{q_2}\right)Q\left(\frac{p_1}{q_1}\right)$$

として，右辺第 1 式は $F(x)$ が α で多くの零をもつことから p_1/q_1 を α に十分近くとることによって極めて小さくなり，第 2 式は $\alpha-p_2/q_2$ をさらに十分小さくとることによって極めて小さくなり，合わせて γ が極めて小さくなることを示して矛盾を得る．

注．(1) の解の分母は常に正であるとする．

次の Siegel の補題はよく知られている．証明は部屋割り論法による．例えば，W.M.Schmidt, Diophantine Approximation, Springer L.N.M.785, Lemma 5B, p.127 にあるが，ここにも証明を付ける．

Siegel の補題　$N>M\geqq 1$ とするとき，未知数の個数が N，方程式の個数が M の整数係数連立 1 次方程式

$$\sum_{i=1}^{N}a_{ij}x_i=0\quad(j=1,\cdots,M)$$

には非自明な整数解で

$$|\text{解}|\leqq(N\max\{|a_{ij}|\})^{M/(N-M)}$$

なるものがある．

証明　$N>M$ より非自明な解は存在する．

$$y_j=\sum_{i=1}^{N}a_{ij}x_i\quad(j=1,\cdots,M)$$

とおき，これを N 次元空間の各座標が整数である格子点から M 次元空間の格子点への写像とみる．$A=\max\{|a_{ij}|\},\ X=[(NA)^{M/(N-M)}]$ とおく．$(x_1,\cdots,x_N)$ は $0\leqq x_i\leqq X$ なる格子点を動くとする．$-B_j,\ C_j$ をそれぞれ係数 $a_{ij}\ (1\leqq i\leqq N)$ の負なるものおよび正なるものの和とする．像の y_j は

$$-B_jX\leqq y_j\leqq C_jX$$

を満たす．$B_j+C_j \leqq NA$ なので，像 $(y_1,\cdots,y_M)$ は一辺の長さが NAX の M 次元立方体に入る．その格子点の個数 $\leqq (NAX+1)^M$．一方，動ける $(x_1,\cdots,x_N)$ の個数は $(X+1)^N$．ところが，$X+1>(NA)^{M/(N-M)}$ より

$$(NAX+1)^M<(NA)^M(X+1)^M<(X+1)^{N-M}(X+1)^M=(X+1)^N$$

であるから，動ける点の個数が像がとり得る点の個数より多いから，少なくとも二つの相異なる点 $(x_i^{(1)}),\ (x_i^{(2)})$ が存在してその像は一致する．$x_i=x_i^{(1)}-x_i^{(2)}$ とおけば補題の非自明な解となる．

次は代数体の基底をとり整数係数方程式に書き直せばよい．

Siegel の補題′　K を次数 d の代数体とし，$N>dM$ とするとき，未知数の個数が N，方程式の個数が M なる，K の代数的整数を係数とする連立 1 次方程式

$$\sum_{i=1}^{N}\alpha_{ij}x_i=0 \quad (j=1,\cdots,M)$$

に対して，K のみによって決まる定数 c があって，非自明な有理整数解で

$$|\text{解}|\leqq(cN\max\{\overline{|\alpha_{ij}|}\})^{dM/(N-dM)}$$

なるものがある．ここで $\overline{|\alpha|}$ は α の共役の絶対値の最大値を表す．

Thue の定理の証明　$0<\theta<1$ とする．(後で $\theta\to 0$ とする.)　以下，定数 $c_1,\ c_2,\ldots$ は α のみによる．

Lemma 1 (補助関数の構成)　$c_1>0$ があって，任意の自然数 N に対し，$M=[(1+\theta)dN/2]\ (<dN)$ とおくと，高々M 次の整数係数多項式 $P(x)=\sum_{i=0}^{M}a_ix^i,\ Q(x)=\sum_{i=0}^{M}b_ix^i$ で

$$|a_i|,\ |b_i|\leqq c_1^{N/\theta} \quad (i=0,\cdots,M)$$

を満たし，かつ

$$F(x)=P(x)-\alpha Q(x)$$

が $x=\alpha$ で少なくとも N 位の零点をもつもの，すなわち

$$F^{(k)}(\alpha)=0,\quad 0\leqq k\leqq N-1, \tag{2}$$

となるものがある．

証明　条件 (2) は

$$\frac{a^{M+1}}{k!}F^{(k)}(\alpha)=\frac{a^{M+1}}{k!}\left(\sum_{k\leqq i\leqq M}a_ii(i-1)\cdots(i-k+1)\alpha^{i-k}\right.$$

$$\left.-\alpha\sum_{k\leqq i\leqq M}b_ii(i-1)\cdots(i-k+1)\alpha^{i-k}\right)=0, \tag{3}$$

$$0\leqq k\leqq N-1$$

となる．ここで，$a\in\mathbf{Z},\ a\alpha\in\mathcal{O}_K(K\text{ の整数環}),\ K=\mathbf{Q}(\alpha)$．
a_i,b_i: 未知数，　その個数 $=2(M+1)$
方程式の個数 $=N$

$\overline{|\text{係数}|} \leqq c'^M$　$\because$) $\binom{i}{k} \leqq 2^i \leqq 2^M$.
Siegel の補題′より

$$\begin{aligned} |\text{解}| &\leqq (c \cdot 2(M+1)c'^M)^{dN/(2(M+1)-dN)} \\ &\leqq (c''^M)^{dN/((1+\theta)dN-dN)} \\ &\leqq (c''^{(1+\theta)dN/2})^{1/\theta} \leqq c_1^{N/\theta} . \end{aligned}$$

さて，この $P(x),\ Q(x)$ は一方が他方の定数倍とはなっていない．
$\because$)　$P(x) = cQ(x)$ と仮定する．$c \in \mathbf{Q}$ である．よって $F(x) = (c-\alpha)Q(x),\ c-\alpha \neq 0.\ F(x)$ は $x = \alpha$ で N 位の零をもつから，$Q(x)$ は $(x-\alpha)^N$ で割れる．したがって，$Q(x)$ は α の定義多項式の N 乗で割れる．よって次数の比較から $dN \leqq M$ となるが，これは M の決め方に反する．

そこで

$$W(x) = P(x)Q'(x) - P'(x)Q(x)$$

とおく．$W(x)$ は Wronski 行列式と呼ばれるものである．上のことから $W(x) \not\equiv 0$ である．また $W(x)$ は整数係数の高々 $2M-1$ 次の多項式である．

Lemma 2　$c_2 > 0$ があって，任意の有理数 p_1/q_1 に対し，

$$s = \mathrm{ord}_{x=\frac{p_1}{q_1}} W(x) < c_2 \frac{N}{\theta \log q_1} . \tag{4}$$

さらに，0 でない任意の有理数 p_2/q_2 に対し，$l \leqq s+1$ なる l があって

$$\gamma = \frac{1}{l!}\left(P^{(l)}\left(\frac{p_1}{q_1}\right) - \frac{p_2}{q_2}Q^{(l)}\left(\frac{p_1}{q_1}\right)\right) \neq 0. \tag{5}$$

証明　零点の位数の定義より，$W(x)$ は $(x-p_1/q_1)^s$ で丁度割れるが，Gauss の補題より

$$W(x) = (q_1x - p_1)^s R(x), \quad R \in \mathbf{Z}[x]$$

と書ける．すると，

$$|W(x) \text{ の最高次の係数 }| \geqq q_1^s .$$

一方，この左辺 $\leqq 2M \cdot Mc_1^{2N/\theta}$.

$$\therefore\ s\log q_1 \leqq \log 2 + 2\log M + \frac{2N}{\theta}\log c_1 < c_2\frac{N}{\theta}.$$

よって (4).
後半については，s の定義と，Leibniz の公式より，

$$0 \neq W^{(s)}\left(\frac{p_1}{q_1}\right) = \sum_{i=0}^{s}\binom{s}{i}\begin{vmatrix} P^{(i)}(p_1/q_1) & Q^{(i)}(p_1/q_1) \\ P^{(s-i+1)}(p_1/q_1) & Q^{(s-i+1)}(p_1/q_1) \end{vmatrix}.$$

もしすべての $0 \leqq i \leqq s+1$ について，$P^{(i)}(p_1/q_1) - \frac{p_2}{q_2}Q^{(i)}(p_1/q_1) = 0$ であれば上の右辺の行列式はすべて 0 になってしまうので，ある $0 \leqq l \leqq s+1$ があって

$$\gamma = \frac{1}{l!}\left(P^{(l)}\left(\frac{p_1}{q_1}\right) - \frac{p_2}{q_2}Q^{(l)}\left(\frac{p_1}{q_1}\right)\right) \neq 0.$$

γ は有理数であるが，P, Q の次数が M であることより，(5) の分母の大きさをみると，γ は小さくなれない．すなわち

Lemma 3　$|\gamma| \geqq \dfrac{1}{q_1^{M-l} q_2}$.

証明　(5) より．

一方 F は $x=\alpha$ で零を沢山もち，l が小となる状況の下では，l 回微分しても零は沢山余っていて，$p_1/q_1,\ p_2/q_2$ が α に近いと γ は小となる．これは矛盾を導く．これを見るために

$$\begin{aligned}
\gamma &= \frac{1}{l!}\left(P^{(l)}\left(\frac{p_1}{q_1}\right) - \frac{p_2}{q_2}Q^{(l)}\left(\frac{p_1}{q_1}\right)\right) \\
&= \frac{1}{l!}\left(P^{(l)}\left(\frac{p_1}{q_1}\right) - \alpha Q^{(l)}\left(\frac{p_1}{q_1}\right)\right) + \frac{1}{l!}\left(\alpha - \frac{p_2}{q_2}\right)Q^{(l)}\left(\frac{p_1}{q_1}\right) \\
&= \frac{1}{l!}F^{(l)}\left(\frac{p_1}{q_1}\right) + \frac{1}{l!}\left(\alpha - \frac{p_2}{q_2}\right)Q^{(l)}\left(\frac{p_1}{q_1}\right)
\end{aligned} \tag{6}$$

と変形する．はじめに評価の大まかな方針を述べる．(6) の第 1 項については，F は $x=\alpha$ で N 位の零をもつので，Taylor 展開すると

$$F(x) = \frac{F^{(N)}(\alpha)}{N!}(x-\alpha)^N + \cdots.$$

よって

$$F^{(l)}(x) = \frac{N\cdots(N-l+1)}{N!}F^{(N)}(\alpha)(x-\alpha)^{N-l} + \cdots.$$

N が大きく l が小さい状況の下では，p_1/q_1 が α に十分近いと

$$F^{(l)}\left(\frac{p_1}{q_1}\right) = \frac{N\cdots(N-l+1)}{N!}F^{(N)}(\alpha)\left(\frac{p_1}{q_1}-\alpha\right)^{N-l} + \cdots$$

は非常に小さくなる．また，(6) の第 2 項については，p_2/q_2 を α にさらに近くとることによって第 1 項と同じほど小さくすることができる．以下これをより詳細にみる．

Lemma 4　$c_3 > 0$ があって，$l < N$ となっているならば，(1) の任意の解 $p_1/q_1,\ p_2/q_2$ に対し，

$$|\gamma| < c_3^{N/\theta}\max\left\{\frac{1}{q_1^{(N-l)\rho}}, \frac{1}{q_2^{\rho}}\right\}.$$

ただし，

$$\rho = \frac{d}{2} + 1 + \varepsilon.$$

証明　(6) の第 1 項について．$F(x)$ を $x=\alpha$ において Taylor 展開すると

$$F(x) = \sum_{N\leqq k\leqq M}\frac{F^{(k)}(\alpha)}{k!}(x-\alpha)^k,$$

ゆえに

$$F^{(l)}(x) = \sum_{N\leqq k\leqq M}\frac{k\cdots(k-l+1)}{k!}F^{(k)}(\alpha)(x-\alpha)^{k-l}.$$

よって

$$(6)\text{ の第 1 項} = \sum_{N\leqq k\leqq M}\binom{k}{l}\frac{1}{k!}F^{(k)}(\alpha)\left(\frac{p_1}{q_1}-\alpha\right)^{k-l}.$$

これを上から評価する．$\sum$ は M 個以下の和，$\binom{k}{l} \leqq 2^M$，$F^{(k)}(\alpha)$ の項の個数 $\leqq 2(M+1)$，$\frac{1}{k!}x^i$ の k 階微分によって出てくる係数は $\frac{i\cdots(i-k+1)}{k!} \leqq 2^M$，$F$ の係数は $|a_i|, |b_i| \leqq c_1^{N/\theta}$，$\alpha$ のべきは高々 $M+1$．したがって

$$|(6) \text{ の第 } 1 \text{ 項 }| \leqq M4^M \cdot 2(M+1)c_1^{N/\theta}(\max\{|\alpha|, 1\})^{M+1} \cdot \frac{1}{q_1^{\rho(N-l)}}$$

を得る．(6) の第 2 項については Taylor 展開せずに直接評価する．$Q^{(l)}(p_1/q_1)$ の項の個数 $\leqq (M+1)$，$\frac{1}{l!}x^i$ の l 階微分によって出てくる係数は $\frac{i\cdots(i-l+1)}{l!} \leqq 2^M$，$Q$ の係数は $|b_i| \leqq c_1^{N/\theta}$，$|p_1/q_1| < |\alpha| + 1$ としてよく，そのべきは高々 M．したがって

$$|(6) \text{ の第 } 2 \text{ 項 }| < (M+1)2^M c_1^{N/\theta}(|\alpha|+1)^M \cdot \frac{1}{q_2^{\rho}}$$

となる．この二つを合わせて，

$$|\gamma| < c_3^{N/\theta} \max\left\{ \frac{1}{q_1^{(N-l)\rho}}, \frac{1}{q_2^{\rho}} \right\}.$$

さて，(1) は無限個の解をもつ，と仮定する．そして矛盾を導く．
(以後の計算から必要になることが分かるのだが) ここで，$\rho = \frac{d}{2} + 1 + \varepsilon$ に対し，$0 < \theta < 1$ を十分小に，N_1 を十分大にとり，

$$\theta > \frac{1}{N_1}$$

かつ

$$\begin{aligned} &(1-\theta)(\rho-1) - \frac{1+\theta}{2}d - \frac{1}{N_1} \\ &= (1-\theta)(\frac{d}{2}+\varepsilon) - \frac{1+\theta}{2}d - \frac{1}{N_1} \\ &= \varepsilon - \theta(d+\varepsilon) - \frac{1}{N_1} > 0 \end{aligned} \tag{7}$$

となるようにする．そして，(1) の解 p_1/q_1 を

$$\frac{c_2}{\theta(\theta - \frac{1}{N_1})} < \log q_1 \tag{8}$$

および

$$\frac{\log c_3}{\theta} < \left((1-\theta)(\rho-1) - \frac{1+\theta}{2}d - \frac{1}{N_1} \right) \log q_1 \tag{9}$$

を満たすようにとる．次に (1) の解 p_2/q_2 を

$$\log q_2 \geqq N_1 \log q_1$$

にとる．そこで $N = [\log q_2 / \log q_1]$ とおく．すなわち，N を

$$q_1^{N+1} > q_2 \geqq q_1^N \tag{10}$$

となるものとする．$N \geqq N_1$ であるから，(7),(8),(9) は N_1 を N で置き換えても成り立っていることに注意する．さて，この N について Lemma 1 の補助関数を作る．(4),(8) より，

$$s < \frac{c_2 N}{\theta \log q_1} < \frac{c_2 N}{\theta} \cdot \frac{\theta(\theta - 1/N)}{c_2} = \theta N - 1,$$

$$\therefore\ l \leqq s + 1 < \theta N. \tag{11}$$

Lemma 3, 4 より，

$$c_3^{N/\theta}\max\left\{\frac{1}{q_1^{(N-l)\rho}},\frac{1}{q_2^{\rho}}\right\} > |\gamma| \geqq \frac{1}{q_1^{M-l}q_2}. \tag{12}$$

(10) より

$$\frac{1}{q_1^{(N-l)\rho}} \geqq \frac{1}{q_1^{N\rho}} \geqq \frac{1}{q_2^{\rho}}.$$

よって (12) は (10) と合わせて

$$\frac{c_3^{N/\theta}}{q_1^{(N-l)\rho}} > |\gamma| \geqq \frac{1}{q_1^{M-l}q_2} > \frac{1}{q_1^{M-l}q_1^{N+1}}. \tag{13}$$

となる．ゆえに，(11) および $M=[(1+\theta)dN/2] \leqq (1+\theta)dN/2$ より

$$\begin{aligned} c_3^{N/\theta} &> q_1^{(N-l)\rho-M+l-N-1} \\ &= q_1^{(N-l)(\rho-1)-M-1} \\ &> q_1^{(N-\theta N)(\rho-1)-M-1} \\ &\geqq q_1^{(N-\theta N)(\rho-1)-\frac{1+\theta}{2}dN-1} \\ &= q_1^{((1-\theta)(\rho-1)-\frac{1+\theta}{2}d-1/N)N}. \end{aligned}$$

これは (9) に矛盾する．この矛盾は (1) が無限個の解をもつと仮定したことから生じた．よって，(1) は有限個の解しかもたない．

定理の証明終り