Integral points and the rank of Thue elliptic curves over number fields

児島 道隆 (早稲田大学)

概 要

楕円曲線の有理点に関して最も基本的な結果は, Mordell-Weil の定理と Siegel の定理である. Mordell-Weil の定理は, 代数体上定義された楕円曲線の有理点の全体が有限生成アーベル群をなすことを主張する. 一方, Siegel の定理は, 代数体上定義された楕円曲線の任意のアフィンモデルにおける整点の個数が有限個であることを主張する. 本報告では, 代数体上定義された楕円曲線の整点の個数を, ランクに関する式で上から評価する問題を扱う.

1 有理数体上での問題の定式化

$f(x,y) \in \mathbb{Z}[x,y]$ を有理整数係数の 3 次同次式で, 判別式が 0 でないものとする. ここで, $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ とおくとき, $f(x,y)$ の判別式は,

$$\mathrm{disc}(f) = -27a^2d^2 - 4ac^3 + 18abcd - 4b^3d + b^2c^2$$

で与えられる.

各 0 でない整数 m に対し, 曲線 C_m を

$$C_m : f(x,y) = mz^3$$

で定義する. また, Thue 方程式 $f(x,y) = m$ の整数解の個数を $N_f(m)$ とおく.

$$N_f(m) = \#\{(x,y) \in \mathbb{Z}^2 | f(x,y) = m\}.$$

曲線 C_m は種数 1 を持つ. ここで, 曲線 C_m が少なくとも 1 つ $\mathbb{Q}$-有理点を持つと仮定する. すると, C_m は $\mathbb{Q}$ 上定義された楕円曲線の構造を持つ. このとき, Mordell-Weil の定理は次のように述べられる.

定理 1.1 ([7] Theorem VIII.4.1). 曲線 C_m の $\mathbb{Q}$-有理点全体の集合 $C_m(\mathbb{Q})$ は有限生成アーベル群をなす.

一方, Thue は 1909 年に Thue 方程式の整数解の個数に関する基本的な結果を証明している.

定理 1.2 ([7] Exercise IX.9.6). Thue 方程式 $f(x,y) = m$ の整数解の個数 $N_f(m)$ は高々有限個である.

定理 1.1 と定理 1.2 より, Thue 方程式 $f(x,y) = m$ に関して, その整数解の個数 $N_f(m)$ と, 楕円曲線 C_m のランク $\mathrm{rank}(C_m(\mathbb{Q}))$ という 2 つの量が定まる. そこで, これらの 2 つの量の関係を考えてみたい. 具体的には, 整点の個数 $N_f(m)$ を $\mathrm{rank}(C_m(\mathbb{Q}))$ の式で上から評価する問題を考える. このような問題は J. Silverman によって始められている.

定理 1.3 ([5]). 絶対的な定数 $\kappa > 0$ と, 同次式 $f(x,y)$ のみに依存する定数 $m_0 > 0$ があり, $|m| > m_0$ を満たす全ての cube-free な整数 m に対し,

$$N_f(m) < \kappa^{\mathrm{rank}(C_m(\mathbb{Q}))+1}$$

が成立する.

この問題に関連して, 次の問題が考えられる.

問題 1.4. $\mathrm{disc}(f) \neq 0$ であり,

$$\sup_{m:cube-free} N_f(m) = \infty$$

を満たすような 3 次同次式 $f(x,y) \in \mathbb{Z}[x,y]$ は存在するか？

もし, このような 3 次同次式が存在するのであれば, 定理 1.3 より, 有理数体 $\mathbb{Q}$ 上定義された, ランクのいくらでも大きい楕円曲線が存在するという予想が肯定的に解決されることになる. しかしながら, 実際には $f(x,y) = m$ の整数解の個数 $N_f(m)$ が大きくなるような同次式 $f(x,y)$ と整数 m の組を見つけるのは非常に難しい.

表 1 は, 同次式 $f(x,y) = x^3 + y^3$ を固定し, m を 1 から 15000 まで動かして, $N_f(m)$ がどのように振る舞うかを示したものである.

また, 次ページの表 2 は $f(x,y) = x^3 + xy^2$ に関するものである.

表 1: $f(x,y) = x^3 + y^3$

m の範囲	$\max(N_f(m))$	最大値を与える m
1〜1000	6	728
1001〜2000	4	1027,1216,...,1729
2001〜3000	4	2457
3001〜4000	6	3367
4001〜5000	6	4104
5001〜6000	6	5824,5859
6001〜7000	4	6832
7001〜8000	4	7657,7992
8001〜9000	4	8216,8587,8911
9001〜10000	4	9728,9919
10001〜11000	4	10621,10712
11001〜12000	4	11375
12001〜13000	4	12096,12663,...
13001〜14000	4	13832,13851,...
14001〜15000	4	14911

$N_f(m)$ は非常に小さい値を取る傾向にあるが, J. Silverman により, m が cube-free であるという制限を外せば, 任意の 3 次同次式 $f(x,y)$ に対し, $N_f(m)$ はいくらでも大きくなりうることが示されている.

表 2: $f(x,y)=x^3+xy^2$

m の範囲	$\max(N_f(m))$	最大値を与える m
1〜1000	6	170,730
1001〜2000	6	1160,1360
2001〜3000	6	2210
3001〜4000	8	3250
4001〜5000	6	4240,4590
5001〜6000	6	5840
6001〜7000	6	6970
7001〜8000	4	7290,7397,7696
8001〜9000	6	8720
9001〜10000	6	9280
10001〜11000	6	10880
11001〜12000	4	11310
12001〜13000	4	12560
13001〜14000	6	13130
14001〜15000	4	14040,14310,...

定理 1.5 ([6]). $f(x,y)\in\mathbb{Z}[x,y]$ を 3 次同次式で, 判別式が 0 でないものとする. このとき, $f(x,y)$ のみに依存する定数 $c=c(f)>0$ が存在して, 無限個の整数 m に対し,

$$N_f(m)>c\sqrt[3]{|m|}$$

が成立する.

2 一般の代数体への拡張

J. Silverman の定理 1.3 を任意の代数体に拡張することを考える.

K を代数体とし, $f(x,y)\in\mathfrak{o}_K[x,y]$ を K の整数を係数とする 3 次同次式で, 判別式が 0 でないものとする. 各 $0\neq\beta\in\mathfrak{o}_K$ に対し, 曲線 C_β を

$$C_\beta : f(x,y)=\beta z^3$$

で定義する. また, Thue 方程式 $f(x,y)=\beta$ の K の整数解の個数を $N_f(\beta)$ とおく.

$$N_f(\beta)=\#\{(x,y)\in\mathfrak{o}_K^2 | f(x,y)=\beta\}$$

このとき, 曲線 C_β は種数 1 を持ち, $N_f(\beta)>0$ の下で C_β は K 上定義された楕円曲線の構造を持つ. 一般の代数体上でも, 初めのセクションで紹介した基本的な定理が成り立つ.

定理 2.1 ([7] Theorem VIII.6.7). 曲線 C_β の K-有理点の全体 $C_\beta(K)$ は有限生成アーベル群の構造を持つ.

定理 2.2 ([7] Corollary IX.3.2.2). Thue 方程式 $f(x,y)=\beta$ の K の整数解の個数 $N_f(\beta)$ は高々有限個である.

さて, 定理 1.3 には整数 m が cube-free であるという条件が含まれている. 定理 1.3 を一般の代数体に拡張するため, 一般の代数体においても, cube-free という概念を定義しなければならない. これは次のように定義する. すなわち, 整数 $\beta \in \mathfrak{o}_K$ が cube-free であるとは, β で生成される $\mathfrak{o}_K$ のイデアル (β) が cube-free, つまり素イデアルの 3 乗で割れないことと定める.

このとき, 我々の問題は次のように定式化される. 問題は以下の結果より予想と呼んでよい.

予想 2.3. 代数体 K のみに依存する定数 $\kappa = \kappa(K) > 0$ と, 代数体 K と同次式 $f(x, y)$ に依存する定数 $M = M(K, f) > 0$ が存在して, $H_K(\beta) \geq M$ であるような全ての cube-free である整数 $\beta \in \mathfrak{o}_K$ に対し,

$$N_f(\beta) < \kappa^{\operatorname{rank} C_\beta(K)+1}$$

が成立する. ここで, H_K は代数体 K に関する高さ関数であり, その定義は後で述べる.

本報告の主結果は, 予想 2.3 が全ての虚 2 次体に対して正しいことを主張する.

定理 2.4 ([2]). K を虚 2 次体とし, $f(x, y)$ を K の整数を係数とする 3 次同次式で, 判別式が 0 でないものとする. そして, $C_\beta, N_f(\beta)$ を前のように定める. このとき, 体 K のみに依存する定数 $\kappa = \kappa(K) > 0$ と, 体 K と同次式 $f(x, y)$ に依存する定数 $M = M(K, f) > 0$ が存在して, $H_K(\beta) \geq M$ であるような全ての cube-free な整数 $\beta \in \mathfrak{o}_K$ に対し,

$$N_f(\beta) < \kappa^{\operatorname{rank} C_\beta(K)+1}$$

が成立する.

定理 2.4 においては, 定数 κ は体 K のみに依存するものとなっている. ここで, もし定数 κ を体 K だけでなく, 同次式 $f(x, y)$ にも依存することを許すのであれば, 予想 2.3 は任意の代数体で成り立つというのが, 次の結果である.

定理 2.5 ([3]). K を任意の代数体とし, $f(x, y)$ を K の整数を係数とする 3 次同次式で, 判別式が 0 でないものとする. このとき, 体 K と同次式 $f(x, y)$ に依存する定数 $\kappa = \kappa(K, f) > 0$ が存在して, 全ての cube-free な整数 $\beta \in \mathfrak{o}_K$ に対し,

$$N_f(\beta) < \kappa^{\operatorname{rank} C_\beta(K)+1}$$

が成立する.

3 高さ関数の定義と性質

定義. K を代数体とし, M_K を K の素点の全体の集合とする. 各 $v \in M_K$ に対し, $|\cdot|_v$ によって, v に属する正規化された付値を表す. ここで, 正規化された付置とは, 有理数体 $\mathbb{Q}$ 上に制限した時に, $\mathbb{Q}$ の正規化された付置の 1 つと一致するもののことを指す. また, $n_v = [K_v : \mathbb{Q}_v]$ を局所次数とする.

さて, $P \in \mathbb{P}^N(K)$ を同次座標で

$$P = [x_0, \cdots, x_N], \quad (x_i \in K)$$

と書くとき, K に関する P の高さは,

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \cdots, |x_N|_v\}^{n_v}$$

と定義される. また, P の絶対的高さは,

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}$$

と定義される. そして, P の絶対的対数的高さは,

$$h(P) = \log H(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{\log |x_0|_v, \cdots, \log |x_N|_v\}$$

と定義される.

今までは, 射影空間上の点に対し, 高さを定義してきたが, 代数的数に対してもその高さを定義したい.

$x \in K$ に対し, K に関する x の高さは,

$$H_K(x) = H_K([x,1]) = \prod_{v \in M_K} \max\{|x|_v, 1\}^{n_v}$$

と定義される. また, x の絶対的高さは,

$$H(x) = H_K(x)^{1/[K:\mathbb{Q}]}$$

で定義される. そして, x の絶対的対数的高さ関数は,

$$h(x) = \log H(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{\log |x|_v, 0\}$$

で定義される.

今度は, 楕円曲線上の点に対して, 高さ関数を定義したい. E/K を代数体 K 上定義された楕円曲線とし, $f \in \overline{K}(E)$ を定数でない偶関数とする. このとき, 各 $P \in E(\overline{K})$ に対し, f に関する P の絶対的対数的高さは,

$$h_f(P) = h(f(P))$$

で定義される.

そして, P の標準的高さは,

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{n \to \infty} 4^{-n} h_f([2^n]P)$$

で定義される.

次に, 高さ関数の持つ性質をいくつか挙げる.

命題 3.1 ([7] Theorem VIII.5.11). K を代数体とし, $C > 0$ とする. このとき,

$$\#\{P \in \mathbb{P}^N(K) | H_K(P) < C\} < \infty$$

が成り立つ.

命題 3.2 ([7] Theorem VIII.9.3). E/K を代数体 K 上定義された楕円曲線とし, $P \in E(K)$ とする. このとき,

$$\hat{h}(P) = 0 \iff P \in E(K)_{tor}$$

が成り立つ.

命題 3.3 ([7] Proposition VIII.9.6). E/K を代数体上定義された楕円曲線とする. このとき, 標準的高さ関数 $\hat{h}$ は格子 $E(K)/E(K)_{\mathrm{tor}}$ 上の正値 2 次形式を定義する.

命題 3.4 ([4]). E/K を代数体 K 上定義された楕円曲線とし, E の j-不変量 j_E が K の整数であるとする. このとき, $[K:\mathbb{Q}]$ のみに依存する定数 $c>0$ が存在して, 全てのねじれ元でない点 $P \in E(K)$ に対し,

$$\hat{h}(P) > c\max(h(j_E), \log N_{K/\mathbb{Q}}(\mathfrak{D}_{E/K}), 1)$$

が成立する. ここで, $\mathfrak{D}_{E/K}$ は E/K の minimal discriminant である.

命題 3.5 ([7] Theorem VIII.9.3, Excercise VIII.8.18). E/K を代数体 K 上定義された楕円曲線とし, そのワイエルシュトラス方程式を,

$$E : y^2 = x^3 + Ax + B$$

とする. このとき, 関数 x に関する高さと標準的高さの間には次の関係が成立する:

$$2\hat{h}(P) - h_x(P) = O(1).$$

ここで, $O(1)$ は有界な関数を表す.

より正確に, 絶対的な定数 $c_1, c_2 > 0$ が存在し, 全ての $P \in E(\overline{K})$ に対し,

$$|2\hat{h}(P) - h_x(P)| < c_1 h([A, B, 1]) + c_2$$

が成立する.

命題 3.6 ([5] Lemma 6). V をランク r の自由アーベル群とし, Q を V 上の正値 2 次形式とする. そして,

$$A = \min(Q(a) | 0 \neq a \in V)(> 0)$$

とおく. このとき, 定数 $B > 0$ に対し,

$$\#\{a \in V | Q(a) < B\} < \left(2\sqrt{\frac{B}{A}} + 1\right)^r$$

が成立する.

4 定理 2.5 の証明の方法

このセクションでは, 主定理 2.5 の証明に用いる道具を紹介する.

I. 曲線 C_β のヤコビアン

曲線 C_β のヤコビアンは, 次のワイエルシュトラスモデルを持つ:

$$y^2 = x^3 - 432\beta^2 D.$$

ここで, D は同次式 $f(x, y)$ の判別式である.

II. quasi-minimal 方程式
代数体 K 上定義された楕円曲線 E/K のワイエルシュトラス方程式

$$y^2 = x^3 + Ax + B$$

が quasi-minimal であるとは, E を定義するモデルの中で $A, B \in \mathfrak{o}_K$ であって, $|N_K(4A^3 + 27B^2)|$ が最小であるもののことである.

III. covariant polynomials
$f(x, y) \in \mathfrak{o}_K[x, y]$ を 3 次同次式で, 判別式が 0 でないものとし, それを具体的に

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \quad (a, b, c, d \in \mathfrak{o}_K)$$

と書く. このとき, 同次式 $f(x, y)$ の次数 2,3 の covariant polynomial は, 次の式でそれぞれ定義される:

$$\begin{aligned} G(x, y) &= (3ac - b^2)x^2 + (9ad - bc)xy + (3bd - c^2)y^2, \\ H(x, y) &= (27a^2d - 9abc + 2b^3)x^3 - 3(6ac^2 - b^2c - 9abd)x^2y \\ &\quad +3(6b^2d - bc^2 - 9acd)xy^2 - (27ad^2 - 9bcd + 2c^3)y^3. \end{aligned}$$

IV. Silverman の結果
ワイエルシュトラス方程式によって定義された楕円曲線に関しても, 予想 2.3 と類似の結果が J. Silverman によって得られている. 定理 2.5 の証明では, 曲線 C_β からそのヤコビアンへ morphism を作り, J. Silverman の結果を適用する.

5 定理 2.4 の証明

定理 2.4 の証明は 3 つのステップから成る.

Step 1. このステップでは, Thue 方程式の整数解の高さの上界を与える. 証明するのは, 次の命題 5.1 である.

命題 5.1. K を虚 2 次体とし, $f(x, y) \in \mathfrak{o}_K[x, y]$ を 3 次同次式で, 判別式が 0 でないものとする. このとき, 体 K のみに依存する定数 $c > 0$ と, 同次式 $f(x, y)$ に依存する定数 $\gamma > 0$ が存在して, 全ての 0 でない整数 $\beta \in \mathfrak{o}_K$ に対し, Thue 方程式 $f(x, y) = \beta$ の K の整数解 (x, y) は,

$$H(x), H(y) < \gamma H(\beta)^c$$

を満たす.

Step 2. このステップでは, 楕円曲線の族

$$E_D : y^2 = x^3 + D$$

について考察し, それらの有理点のうち高さがある式で上から押さえられる点の個数の上界を求める.

命題 5.2. K を虚 2 次体とする. また, $0 \neq D \in \mathfrak{o}_K, c > 0, \gamma \in \mathbb{R}$ が与えられているものとする. このとき, 体 K のみに依存する定数 $c_1, c_2, c_3 > 0$ と, D, c, γ に依存する定数 $M > 0$ が存在し, $H_K(\beta) \geq M$ を満たす全ての sixth-power-free な整数 $\beta \in \mathfrak{o}_K$ に対し,

$$\#\{P \in E_{\beta D}(K) | h_x(P) < c\, h(\beta) + \gamma\} < c_1(c_2\sqrt{c + c_3} + 1)^{\operatorname{rank} E_{\beta D}(K)}$$

が成立する.

Step 3. 最後のステップでは, Thue 方程式からそのヤコビアンへ morphism を作る. そのヤコビアンは E_D 型のモデルを持つので, 前の 2 つのステップを組み合わせることにより, 定理 2.4 の証明が完了する.

本報告では, 最後にこれら 3 つのステップのうち, K が虚 2 次体であることを最も使っているステップ 1 について, 詳細を述べることにする.

命題 5.1 の証明.

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \quad (a, b, c, d \in \mathfrak{o}_K)$$

と書く. 今から, 体 K のみに依存する定数 $c' > 0$ と, 同次式 f に依存する定数 $\gamma' > 0$ が存在して,

$$x, y \in o_K\,,\, f(x, y) \neq 0 \implies H(f(x, y)) > \gamma' \max(H(x), H(y))^{c'} \tag{A}$$

が成立することを示すことにする. これが示されれば, この不等式に Thue 方程式 $f(x, y) = \beta$ を代入することにより, 目標の結果を得ることができる. 今回は, $y \neq 0, H(x) \leq H(y)$ と仮定して, 議論を進めることにする. ここで, $f(x, 1)$ の異なる 3 つの根を $\zeta_1, \zeta_2, \zeta_3 \in \mathbb{C}$ とする. このとき,

$$f(x, y) = ay^3\Big(\frac{x}{y} - \zeta_1\Big)\Big(\frac{x}{y} - \zeta_2\Big)\Big(\frac{x}{y} - \zeta_3\Big)$$

が成立する. 今, $\Delta = \min\{|\zeta_i - \zeta_j|\ |i \neq j\}$ を $f(x, 1)$ の異なる根の差の絶対値の最小値とする. もし, $\left|\dfrac{x}{y} - \zeta_i\right| > \dfrac{\Delta}{2}\ (i = 1, 2, 3)$ であれば, この式より,

$$H(f(x, y)) = |f(x, y)| > |a|\Big(\frac{\Delta}{2}\Big)^3 H(y)^3.$$

となるから, $c' = 3, \gamma' = |a|\left(\dfrac{\Delta}{2}\right)^3$ と取ることができる. 以下では, ある i_0 に対し, $\left|\dfrac{x}{y} - \zeta_{i_0}\right| \leq \dfrac{\Delta}{2}$ である場合について, 考察する. 三角不等式より, $i \neq i_0$ に対しては,

$$\left|\frac{x}{y} - \zeta_i\right| \geq \frac{\Delta}{2}$$

であるから,

$$H(f(x, y)) = |f(x, y)| \geq |a|\left(\frac{\Delta}{2}\right)^2 |y|^3 \left|\frac{x}{y} - \zeta_{i_0}\right| \tag{B}$$

が成立する. 不等式 (A) を示すため, $\left|\dfrac{x}{y} - \zeta_{i_0}\right|$ を下から評価したい. $K = \mathbb{Q}(\omega)$, $(\omega = \sqrt{-m}$, $m \in \mathbb{N})$ と書き, $\frac{x}{y} = c + d\omega$, $(c, d \in \mathbb{Q})$ と表す. また, $1, \omega \in \mathbb{C}$ は $\mathbb{R}$ 上 1 次独立であるから,

$$\zeta_{i_0} = c_{i_0} + d_{i_0}\omega,\ (c_{i_0}, d_{i_0} \in \mathbb{R})$$

と書く. このとき, c_{i_0}, d_{i_0} が代数的数であることは容易に分かる. 次に,

$$\left|\frac{x}{y}-\zeta_{i_0}\right| = \sqrt{(c-c_{i_0})^2+m(d-d_{i_0})^2}$$
$$\geq \max\{|c-c_{i_0}|, |d-d_{i_0}|\} \tag{C}$$

ここで, $c \neq c_{i_0}$ と仮定してよい. 今, $0<\epsilon<1$ を満たす実数 ϵ を 1 つ固定すると, Roth の定理 ([1]) より, 有限個を除く全ての $c \in \mathbb{Q}$ に対し,

$$|c-c_{i_0}| > H(c)^{-(2+\epsilon)}$$

が成立する. よって, 十分に小さい定数 $\gamma_{i_0}>0$ を取れば, 全ての $c_{i_0} \neq c \in \mathbb{Q}$ に対し,

$$|c-c_{i_0}| > \gamma_{i_0} H(c)^{-(2+\epsilon)}$$

が成立する. これを (C) に代入して,

$$\left|\frac{x}{y}-\zeta_{i_0}\right| > \gamma_{i_0} H(c)^{-(2+\epsilon)}$$

となる. 一方,

$$H(c) = H\left(\frac{1}{2}\left(\frac{x}{y}+\overline{\left(\frac{x}{y}\right)}\right)\right) \leq \gamma' H\left(\frac{x}{y}\right) \leq \gamma' \max\{H(x), H(y)\} = \gamma' H(y)$$

が成立する. (全ての $\alpha \in K$ に対し, $H(\alpha)=H(\overline{\alpha})$ であることに注意.) この不等式を一つ前の不等式に代入して,

$$\left|\frac{x}{y}-\zeta_{i_0}\right| > \gamma'_{i_0} H(y)^{-(2+\epsilon)}$$

最後にこの不等式を (B) に代入して,

$$H(f(x,y)) \geq |a|\left(\frac{\Delta}{2}\right)^2 \gamma'_{i_0} H(y)^{1-\epsilon}$$

となり, 不等式 (A) を得る. □

参考文献

[1] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, 1983.

[2] M. Kojima, Integral Points and the Rank of Elliptic Curves over Imaginary Quadratic Fields, Tokyo J. Math. **31** (2008), 175–184.

[3] M. Kojima, Integral Points and the Rank of Thue Elliptic Curves over Number Fields, to appear.

[4] J. Silverman, Lower bound for the canonical height on elliptic curves, Duke Math. J. **48** (1981), 633–648.

[5] J. Silverman, Integer Points and the Rank of Thue Elliptic Curves, Invent. Math. **66** (1982), 395–404.

[6] J. Silverman, Integer points on curve of genus 1, J. London Math. Soc. **28** (1983), 1–7.

[7] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.