Primes of the form $X^3 + NY^3$ and a family of non-singular plane curves which violate the local-global principle (summary)

慶應義塾大学理工学部数学科 *
理化学研究所革新知能統合研究センター数理科学チーム †
平川義之輔
Yoshinosuke Hirakawa
Department of Mathematics, Faculty of Sciences and Technology,
Keio University
Mathematical Science Team,
RIKEN Center for Advanced Intelligence Project

序

本論文では, 著者と清水洋介氏との共同研究に基づいた 2 つのプレプリント [7, 8] の概要を述べる. この共同研究の主結果を端的に述べると,

各自然数 $n \geq 3$ に対して, 有理数体 $\mathbb{Q}$ 上定義された射影的な非特異 n 次平面曲線であって, $\mathbb{Q}$ の各素点 v での完備化 $\mathbb{Q}_v$ 上の有理点を持つにも関わらず $\mathbb{Q}$ 上の有理点は一切持たないものを (無数に) 生成するアルゴリズムを与えた

というものである. 特に, 2 次形式に対する古典的な Hasse の局所大域原理を, 3 変数非特異 n 次形式に対して拡張することはできないであろう, というよく知られた経験則に対して, 構成的な証明を与えた, というのが我々の主結果である.

以下では, この結果の歴史的な位置付けを紹介した上で, 正確な主張とその証明の概要を述べる. 先行研究に関するより詳細な文献表などは, 原論文 [7, 8] を参照していただきたい.

謝辞. 本稿の執筆, 並びに集会における講演の機会をご提供いただきましたオーガナイザーの中村隆氏, 赤塚広隆氏にこの場を借りて深く御礼申し上げます。また, Zoom による快

* 〒223-8522 神奈川県横浜市港北区日吉 3-14-1
† 〒351-0198 埼玉県和光市広沢 2-1

適なリモート講演のサポートをいただきました鈴木雄太氏, 松坂俊輝氏にも, 深く御礼申し上げます. 本稿の元になっている 1 本目の原論文 [7] の共著者である清水洋介氏にも, 貴重な共同研究に導いてくださったことを深く御礼申し上げます. 本研究は日本学術振興会科研費 JP15J05818, 18H05233 に加え, 日本学術振興会拠点形成事業「数論と幾何学を核とする数理科学国際連携拠点形成事業」, 慶應義塾基礎科学・基盤工学インスティテュート（KiPAS）プログラム FY2014-2018, 慶應義塾先端科学技術研究センター（KLL）後期博士課程研究助成金 000036 (2018-2019) 及び 000074 (2019-2020) の援助を受けたものです. また, 本稿の執筆, 並びに集会での講演は, 国際共同利用・共同研究拠点である京都大学数理解析研究所の援助を受けたものです。

1 先行研究

以下, 体 K 上の代数多様体 V に対して, $V(K)$ で V の K 上の有理点全体のなす集合を表す.

まずは, 2 次形式に対する古典的な Hasse の局所大域原理から始める. [*1]

定理 1.1 (Hasse-Minkowski の定理 (cf. [18, Theorem 8, Ch. IV]))**.** $\mathbb{Q}$ 上定義された射影的な 2 次超曲面 $V \subset \mathbb{P}^{d+1}$ $(d \geq 0)$ に対して, 以下の 2 つの条件は同値である.

1. $V(\mathbb{Q}_v) \neq \emptyset$ $(\forall v : \mathbb{Q}$ の素点$)$, *i.e.,* $\mathbb{Q}$ の各素点 v に対して, V は v での完備化 $\mathbb{Q}_v$ 上の有理点を持つ.
2. $V(\mathbb{Q}) \neq \emptyset$, *i.e.,* V は $\mathbb{Q}$ 上の有理点を持つ.

本題に入る前に, 上記の定理の意義を振り返ることで, 有理点問題における局所大域原理の位置付けを確認しておこう. まず, 後半の条件から前半の条件が従うことは自明なので, 定理 1.1 の主張の本質は前半の「局所的な条件」から後半の「大域的な条件」が従う点にある. ここで, 各素点 v ごとには, 中間値の定理や Hensel の補題を適用することで, $V(\mathbb{Q}_v) = \emptyset$ か否かを判定できることを思い出そう. また, Hasse-Weil bound を組み合わせれば, 具体的に計算可能な定数 $c = c(V)$ が存在して, 任意の素数 $p \geq c$ に対して $V(\mathbb{Q}_p) \neq \emptyset$ となることも分かる. 従って, 定理 1.1 は実質的に, **2 次超曲面が有理点を持つか否かを判定するアルゴリズムを与える**. これは, Hilbert の第 10 問題に対する最初の決定的な成果として位置付けられるべきものである.

以上の背景を踏まえると, 定理 1.1 の一般化に関する研究が深まっていくのは, 有理点問題における極めて自然な流れである. しかし, よく知られているように, 高次の超曲面 $V \subset \mathbb{P}^{d+1}$ に対しては, 定理 1.1 の主張そのものを素朴に拡張することはできない.

[*1] 本稿の主題は $\mathbb{Q}$ 上の局所大域原理なので, Hasse-Minkowski の定理も $\mathbb{Q}$ 上に限定した形で述べた.

定理 1.2 ([19])**.** $V \subset \mathbb{P}^2$ を以下の方程式で定義された *3* 次曲線とする.

$$X^3 + 6Y^3 = 10Z^3.$$

この時, 以下が成り立つ.

1. $V(\mathbb{Q}_v) \neq \emptyset$ *(*$\forall v$ *:* $\mathbb{Q}$ *の素点).*
2. $V(\mathbb{Q}) = \emptyset$.

このように, 定理 1.1 の主張の素朴な一般化が成り立たない ($\mathbb{Q}$ 上の) 代数多様体は, ($\mathbb{Q}$ 上の) **局所大域原理の反例**と呼ばれる. 定理 1.2 以外にも, 局所大域原理の反例には様々なものが知られているが, 本稿に直接関係する平面曲線に関する先行研究は [7, 8] でも振り返っているので, ここでは繰り返さない. しかし, 藤原と須藤による以下の具体例は, 上記 Selmer の 3 次曲線を高次化する際の我々の指針であったため, ここで振り返っておくに値する.

定理 1.3 ([5,6])**.** m を非負整数, $V = V_m \subset \mathbb{P}^2$ を以下の方程式で定義された $10m + 5$ 次曲線とする.

$$(X^3 + 5Y^3)(X^2 + XY + Y^2)^{5m+1} = 17Z^{10m+5}.$$

この時, V は局所大域原理の反例である. 即ち, 以下が成り立つ.

1. $V(\mathbb{Q}_v) \neq \emptyset$ *(*$\forall v$ *:* $\mathbb{Q}$ *の素点).*
2. $V(\mathbb{Q}) = \emptyset$.

藤原-須藤 [6] による $V(\mathbb{Q}) = \emptyset$ の証明の手法は,

$$X^3 + 5Y^3 = 17Z^5$$

という一般 Fermat 型方程式が, $\gcd(X, Y, Z) = 1$ となる整数解 (X, Y, Z), 即ち原始解を持たないこと (cf. [5]) に帰着するものである. このような一般 Fermat 型方程式の原始解の非存在そのものは, 係数をうまく取りさえすれば, 3 次体 $\mathbb{Q}(5^{1/3})$ のイデアルや単数に関する Kummer, Dedekind 以来の古典的な手法により示せる. [*2] また, 実は Z^{10m+5} の係数は $53, 89, 131, \ldots$ などと動かすことができる (が, [5,6] ではその無限性には触れていない).

さて, 次章では我々の主結果を述べるが, その前にいくつか注意を述べておこう.

注意 1.4. 1. 定理 1.3 以外にも, 様々な局所大域原理の反例が知られていることは, 上述の通りである. 特に, *3* **次曲線**に関する Poonen の研究 [17], および 4 以上の**偶数** n **次数曲線**に対する比較的最近の Nguyen の一連の研究 [13–15] でも, 非特異平面 n 次

[*2] もちろん, 実際には前半の局所的な条件も成り立つように係数を選ぶ必要があり, 特に [6] では $\mathbb{Q}_3$ 上の解の存在証明に相当な紙数を割いている. このように存在証明が煩雑になる 1 つの理由は, 曲線上の特異点により Hensel の補題を適用する際に必要な 3 進近似計算の精度が上昇するためである (cf. 注意 1.4.2).

曲線型の局所大域原理の反例の無限族が得られている. [*3] また, 既約でない (特に特異点を持つ) 平面曲線に関しては, 定理 1.2 と有理点を持たない 2 次曲線を組み合わせるなどして, 局所大域原理の反例を容易に構成できる.

2. 定理 1.3 の V_m は既約であるが, 非特異なのは $m = 0$ の場合に限り $m > 0$ の場合は常に $[X : Y : Z] = [1 : \zeta_3^e : 0]$ $(e = 1, 2)$ で特異点を持つ. ただし, $\zeta_3 := \exp(2\pi i/3) \in \mathbb{C}$ である. 一方で, 定義方程式の係数の高さに関する密度の意味でも, 平面曲線のモジュライ空間上の自然な位相の意味でも, 特異点を持つ平面曲線は極めて特殊なものに過ぎない. さらに, V_m の定義方程式における Z^{10m+5} の係数 17 を別の非零複素数で置き換えても, 複素代数曲線としては V_m 自身と同型になってしまう. このような複素幾何学的な事情を踏まえると,
   - 非特異平面曲線 (Riemann 面の $\mathbb{Q}$ 上のモデル) に対しては局所大域原理が成り立つのか否か,
   - また Riemann 面として同型でない ($\mathbb{Q}$ 上の) 局所大域原理の反例が無限個存在するか否か,

   を問うことは自然であろう. これが我々の研究の 1 つの動機である (cf. 注意 2.2.4).

2 主結果

注意 1.4.1 を踏まえて, 本稿では奇数 $n \geq 5$ を念頭に置いて, 非特異 n 次平面曲線型の局所大域原理の反例についての成果を紹介する. この場合, 我々の主結果は以下の通りである. 偶数次の場合にも同様の成果はあるが, 詳しくは [8, Theorem 1.2] をご覧いただきたい.

定理 2.1 (cf. [7, Theorem 1.1], [8, Theorem 1.8])**.** 以下のようなアルゴリズムが存在する.

- 入力
  - 奇数 $n \geq 5$.
  - n の素因数 p.
  - $P \not\equiv \pm 1 \bmod 9$ となる整数 $P \in \{p, 2p\}$.
- 出力
  - P にのみ依存する整数 $\iota = \iota_P \in \{1, 2\}$.
  - 整数対の $((n-3)/2)$-組 (b_j, c_j) $(1 \leq j \leq (n-3)/2)$.
  - 素数冪 $L = l^m$ であって, 以下の方程式が定める N 個の平面 n 次曲線が全て非

[*3] ただし, Nguyen の構成は, いずれも超楕円曲線 ($\mathbb{P}^1$ の 2 重被覆) 型の局所大域原理の反例に基づいており, 奇数次平面曲線型の反例構成には応用できそうにない.

特異かつ局所大域原理の反例となるもの.

$$(X^3+P^\iota Y^3)\prod_{j=1}^{(n-3)/2}(b_j^2X^2+b_jc_jXY+c_j^2Y^2)=LZ^n. \tag{1}$$

このアルゴリズムが本稿冒頭の帰結を導くことは, “(無数に) 生成する” という部分を除けば明らかであろうが, この点に関していくつか補足をしておこう.

注意 2.2.

1. 定理 2.1 は, $\iota_P=1$ となる P に対しては [7, Theorem 1.1] で, $\iota_P=2$ となる P に対しては [8, Theorem 1.8] で, それぞれ証明された. 特に, 現時点では, [7] の結果のみから本稿冒頭の結果を導くことは (たとえ奇数次数に限っても) できていない (cf. §4). この場合分けは, 後述の命題 3.3 における場合分けに起因する.
2. 実は, 定理 2.1 のアルゴリズムを反復することで, 出力
   - 整数対の $((n-3)/2)$-組 (b_j,c_j) $(1\le j\le(n-3)/2)$ および
   - 素数冪 L

   を無数に得ることができる. より正確には, 定理 2.1 のアルゴリズムを適切に精密化することで, 任意の正整数 $N_1,N_2>0$ に対して,
   - 整数対の $((n-3)/2)$-組 $(b_{i,j},c_{i,j})$ $(1\le i\le N_1, 1\le j\le(n-3)/2)$ および
   - 素数冪 $L_{i,k}$ $(1\le k\le N_2)$

   を, 以下の方程式が定める N_1N_2 個の平面 n 次曲線が全て非特異かつ局所大域原理の反例となるように出力できる.

$$(X^3+P^\iota Y^3)\prod_{j=1}^{(n-3)/2}(b_{i,j}^2X^2+b_{i,j}c_{i,j}XY+c_{i,j}^2Y^2)=L_{i,k}Z^n. \tag{2}$$

3. 上記非特異代数曲線の複素数体 $\mathbb{C}$ 上の同型類 (Riemann 面の双正則同型類) は $L_{i,k}$ には依存せず, 整数対の $((n-3)/2)$-組 $(b_{i,j},c_{i,j})$ $(1\le j\le N_1)$ のみで決まる. これら $((n-3)/2)$-組 (と 3 次因子 $X^3+P^\iota Y^3$) は, 上記非特異代数曲線を自然に $\mathbb{P}^1$ の $\mathbb{Z}/n\mathbb{Z}$-分岐被覆と見做すことで, $\mathbb{P}^1$ 上の n 点からなる分岐点配置を定める. 逆に, この n 点配置の射影同値類から非特異代数曲線の同型類を復元できる (cf. [12]). 従って, もし出力された N_1 個の $((n-3)/2)$-組 $(b_{i,j},c_{i,j})$ $(1\le i\le N_1)$ が定める分岐点配置の射影同値類が重複しないように $((n-3)/2)$-組 $(b_{i,j},c_{i,j})$ を選ぶことができれば (選び続けられれば), 局所大域原理の反例を与える非特異平面 n 次曲線を無数に得られるが, これは実際に可能である. これで, 本稿冒頭で述べた “無数に生成する” という主張が保証される. 本稿では, 各奇数次数 $n\ge5$ ごとに「局所大域原理の反例を少なくとも 1 つ構成する」という点に焦点を当てるので, 上記議論の詳細は原論文 [7, §4] をご覧いただきたい.

4. 定理 1.3 における藤原-須藤の例と比較することで, 2 次因子を “摂動” することで特異点がスムージングされていることが見て取れるであろう. 実は, このスムージングは特異点の p 進的 (ないし 3 進的) な特異点の変型を組み合わせて得られるものである. このような特異点のスムージングの副次的な恩恵として, 定理 1.3 における藤原-須藤の例に比べて, 局所的な条件が成り立つことの証明も大幅に簡略化できた. このように, 「局所大域原理の反例である」という整数論的な性質を保ったままで特異点をスムージングできるか? という「変型の存在問題」が, 次節で述べるように「ある種の素数が十分豊富に存在すること (素数分布論) 」により肯定的に証明されるという点は, 数論幾何学的に興味深い.

3 証明の概要

この章では, 定理 2.1 の証明の概要を述べる. 代数多様体 V が局所大域原理の反例であることを証明するためには, 当然,

1. $V(\mathbb{Q}_v) \neq \emptyset$ ($\forall v$: $\mathbb{Q}$ の素点) かつ
2. $V(\mathbb{Q}) = \emptyset$

となることを示さねばならない. そのため, 局所大域原理の反例を与える代数多様体の具体的な定義方程式を与えるための素朴な方針としては, 前半の局所的な条件が成り立つような係数に対する十分条件を “十分に” 弱めた上で, これに加えて後半の大域的な条件も成り立つ係数の集合が空にならないように上記十分条件を “程よく” 強めることで, 得られた非空集合から具体的に元を取るのが自然である. この説明だけだとトートロジカルで無意味だが, 以下の命題を通して具体的に説明しよう.

命題 3.1 ([7, Proposition 2.1])**.** *$n \geq 5$ を奇数, p を素数, $P \in \{p, 2p\}$, $\iota \in \{1, 2\}$ とする. b_j, c_j $(1 \leq j \leq (n-3)/2)$, L を, 以下を満たす整数とする.*

1. *各 j に対して, $P^{\iota} b_j^3 + c_j^3$ は P と素な 2 mod 3 型素数である.*
2. *各 j に対して, L は $b_j c_j$ と素である. さらに, L の任意の素因数 l は 2 mod 3 型であり, かつ l^n は L を割り切らない.*
3. *P の任意の 2 mod 3 型素因数 q に対して,*

$$L \equiv \prod_j b_j^2 \not\equiv 0 \bmod q \quad \text{かつ} \quad \sum_j b_j^{-1} c_j \not\equiv 0 \bmod q$$

が成り立つ.

4. $P \not\equiv \pm 1 \bmod 9$ の場合,

$$L \equiv \prod_j b_j^2 \not\equiv 0 \bmod 3 \quad \text{かつ} \quad \sum_j b_j^{-1} c_j \not\equiv 0 \bmod 3$$

が成り立つ.

5. $\gcd(x,y,z) = 1$ かつ $x^3 + P^\iota y^3 = Lz^n$ となる任意の整数の 3 つ組 (x,y,z) に対して, L のある素因数 l が存在して,

$$x \equiv y \equiv 0 \bmod l$$

が成り立つ.

この時, 以下の方程式で定まる射影代数曲線は局所大域原理の反例となる.

$$(X^3 + P^\iota Y^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = LZ^n.$$

命題 3.1 の証明は本稿では述べないが, 重要な点は,

- 条件 1・2 は整数の素因数分解に関する大域的な条件
- 条件 3・4 は $3P$ の素因数に関する局所的な条件
- 条件 5 は不定方程式の原始解に関する大域的な条件

であり,

1. 条件 3・4 は上記代数曲線が $\mathbb{Q}_q$ or $\mathbb{Q}_3$ 上の有理点を持つための条件
2. 条件 1・2・5 は上記代数曲線が $\mathbb{Q}$ 上の有理点を持たないための条件

となっていることである. 局所的な条件を条件 3・4 まで “十分に” 弱めた上で, 条件 1・2・5 で大域的な条件を “程よく” 強めている, というわけである. ここで, $3P$ と素な素数 v に対する $\mathbb{Q}_v$ 上の有理点の存在も気になるであろうが, 実は 6 次拡大 $\mathbb{Q}(\zeta_3, P^{1/3})/\mathbb{Q}$ の Galois 群が 3 次対称群であるという特殊事情により, 方程式 $(X^3 + P^\iota)(X^2 + X + 1) = 0$ は必ず $\mathbb{Q}_v$ $(\gcd(v, 3P) = 1)$ 上の解を持つことが分かる (cf. [5]).

さて, 命題 3.1 の 5 つの条件の中でも, 整数対の $(n-3)/2$-組 (b_j, c_j) に対する条件 1 と, 整数 L に対する条件 5 が一際目を引くであろう. 実際, この 2 つの条件を満たすようなパラメータ b_j, c_j $(1 \le j \le (n-3)/2)$, L の存在証明が, 定理 2.1 の証明の核である.

まず, 条件 1 を満たす整数対の $(n-3)/2$-組 (b_j, c_j) が (無数に) 存在することは, 下記の Heath-Brown と Moroz による素数分布に関する定理の直接的な帰結である.

定理 3.2 ([9, Theorem 1])**.** *f_0 を整数係数の 2 変数既約 3 次形式とし, ρ, γ_1, γ_2 を整数とする. 2 変数 3 次多項式 $f_0(\rho x + \gamma_1, \rho y + \gamma_2)$ の係数の最大公約数を γ_0 とし, $f(x,y) :=$*

$\gamma_0^{-1} f_0(\rho x + \gamma_1, \rho y + \gamma_2)$ とおく．この時，もし $\gcd(f(\mathbb{Z}^{\oplus 2})) = 1$ ならば，$f(\mathbb{Z}^{\oplus 2})$ は無数の素数を含む．

このように，数論幾何的に興味深い対象 (今回の場合は「局所大域原理の反例である」という性質を保った定理 1.3 の例の変型を与えるパラメータ) の存在を証明する，それらの分布を解析する，あるいは具体的に構成するといった際に，特殊な形の素数 (あるいは特殊な形の整数) の分布が鍵になるという観察は，著者にとって興味深い経験であった．

こうして，定理 2.1 の証明の大部分は，以下の命題に帰着される．

命題 3.3 (cf. [7, Proposition 3.3] for $\iota = 1$, [8, Proposition 4.1] for $\iota = 2$)**.** p を素数とし，$P \in \{p, 2p\}$ を $P \not\equiv \pm 1 \bmod 9$ となるように取る．また，3 次体 $K := \mathbb{Q}(P^{1/3})$ の基本単数が $\epsilon = \alpha + \beta P^{1/3} + \gamma P^{2/3}$ となるように整数 α, β, γ を定め，β, γ に応じて ι を以下のように定める．

$$\iota := \begin{cases} 1 & \text{if } \beta \not\equiv 0 \bmod p \text{ または } \beta \equiv \gamma \equiv 0 \bmod p \\ 2 & \text{if } \beta \equiv 0 \bmod p \text{ かつ } \gamma \not\equiv 0 \bmod p \end{cases}.$$

l を P と素な $2 \bmod 3$ 型素数とする．以上の設定の下，さらに，以下の 2 つの条件が成り立つような整数 a, b, c と正整数 m が存在すると仮定する．

1. $l = N_{K/\mathbb{Q}}(a + bP^{1/3} + cP^{2/3})$ $(= a^3 + b^3 P + c^3 P^2 - 3abcP)$.
2. (*a*) $\iota = 1$ の場合，3 つの整数列 $(A_k)_{k\in\mathbb{N}}, (B_k)_{k\in\mathbb{N}}, (C_k)_{k\in\mathbb{N}}$ を

$$A_k + B_k P^{1/3} + C_k P^{2/3} = \epsilon^k (a + bP^{1/3} + cP^{2/3})^m$$

で定めた時，$C_k \equiv 0 \bmod p$ となる自然数 k は存在しない．

(*b*) $\iota = 2$ の場合，bm は p と素である．

この時，p の任意の倍数 $n \geq 3$ と，$\gcd(x, y, z) = 1$ かつ $x^3 + P^\iota y^3 = l^m z^n$ となる任意の整数の 3 つ組 (x, y, z) に対して，

$$x \equiv y \equiv 0 \bmod l$$

が成り立つ．

命題 3.3 において，さらに $m < p$ を仮定すると，その主張は要するに，

一般 *Fermat* 型方程式 $x^3 + P^\iota y^3 = l^m z^p$ は原始解を持たない

ということを言っている．その意味で，命題 3.3 は，藤原-須藤による定理 1.3 の証明に現れた命題

一般 *Fermat* 型方程式 $x^3 + 5y^3 = 17z^5$ は原始解を持たない

の一般化になっている.

命題 3.3 の証明は, 本質的には, Kummer による正則素数 p に対する p 次の Fermat 予想の証明と同様に, 3 次体 $K = \mathbb{Q}(P^{1/3})$ における素数の分解と単数の解析に帰着される. その際, K の類数の p-非可除性が必要になるが, これは

- Dirichlet, Dedekind による解析的類数公式
- Cusick [4, Theorem 3] によるレギュレーターの下界
- Barrucand-Louboutain [3, Corollarie 2] による Dedekind ζ 関数の $s = 1$ での留数の上界
- Barrucand-Cohn [2, Corollary 4.2.1] による純 3 次体の類数の 3-可除性判定法 (cubic rational genus theory の一部)

を組み合わせることで証明できる. 一方, Kummer による Fermat 予想の部分的な証明では, **円単数**に関する非常に精緻な解析が鍵になっており, このことは理論的にも注目に値する事実である. しかし, 今回は, **そのような特殊な単数の解析は不要**である. というより, **そのような精緻な解析を避けるように ι に応じて係数 P^ι を上手く選ぶ**ことが定理 1.3 の定式化に至る鍵であり, 同時に定理 2.1 の証明における技術的なポイントでもある (cf. 予想 4.1). このような “係数を p 進的に揺さぶる” 手法は, Fermat 予想などの与えられた不定方程式の原始解を決定する問題には適用できない. 一方で, 原始解を持たない, あるいは局所大域原理の反例となるような一般 Fermat 方程式を構成する際には, それなりに有効な手法であろうと著者は期待している.

最後に, $\iota = 1$ の場合に命題 3.3 を定理 2.1 に適用するためには, $C_k \equiv 0 \bmod p$ となる自然数 k の非存在を証明する必要があることに注意しよう. これは, $C_k \bmod p$ が k の 2 次式であることに注意すると, その判別式が $\bmod p$ 非平方剰余となることを確かめれば十分である. 従って, (例えば, [16] などの Polya-Vinogradov 型の不等式から得られる) 連続する平方剰余の長さの上界を考慮した上で定理 3.2 を適用することにより, 所望の条件を全て満たす素数冪 $L = l^m = (a^3 + c^3P^2)^m$ の存在を証明できる.

4 Ankeny-Artin-Chowla-Mordell 予想の純 3 次体類似

最後に, 本稿を締め括るにあたって, 興味深い観察を一つ紹介したい.

前章における定理 2.1 の証明では, 命題 3.3 の主張の述べ方, 特に $\iota \in \{1, 2\}$ により場合分けをすることが技術的なポイントである. これに関して, 著者らは以下のような予想を立てた.

予想 4.1 ([7, Conjecture 1.2])**.** *$p \neq 3$ を素数とし, $P \in \{p, 2p\}$ とする. 3 次体 $\mathbb{Q}(P^{1/3})$ の基本単数が $\epsilon = (1/3)(\alpha + \beta P^{1/3} + \gamma P^{2/3}) > 1$ となるように整数 α, β, γ を定める. この時,*

$\beta \neq 0 \bmod p$ が成り立つ. 特に, 素数 $p \neq 3$ に対しては, 定理 *2.1* の $\iota = \iota_P$ は常に $\iota = 1$ と取れる. [*4]

予想 4.1 は, 定理 2.1 の条件付きのアルゴリズム [7] が任意の奇数次数 $n \geq 5$ で適用可能であろうという**希望的観測から生まれたものではない**. これは, 以下の実 2 次体 (或いは**円単数**) に関する古典的な未解決予想の純 3 次体 (或いは $\mathbb{Q}(\zeta_3)$ に付随する**楕円単数**) 類似である.

予想 4.2 ([1] for $p \equiv 1 \bmod 4$, [11] for $p \equiv 3 \bmod 4$)**.** $p \neq 2$ を素数とする. *2* 次体 $\mathbb{Q}(p^{1/2})$ の基本単数が $\epsilon = (1/2)(\alpha + \beta p^{1/2}) > 1$ となるように整数 α, β を定める. この時, $\beta \neq 0 \bmod p$ が成り立つ.

ちなみに, 予想 4.2 は, $p \equiv 1 \mod 4$ の場合は $p < 2 \cdot 10^{11}$ で検証済み [20], $p \equiv 3 \mod 4$ の場合は $p < 10^7$ で検証済み [10] だそうである. 一方, 我々の予想 4.1 は $p < 10^5$ で検証済みである. しかし, この手の予想を数値実験により "信じる" 際には, 以下のことに注意する必要がある. 即ち, $\beta \bmod p$ が $\{0, 1, 2, \ldots, p-1\}$ の各値を取る "確率" が $1/p$ であると仮定すると, $p < X$ の範囲に存在する上記予想の反例の個数は高々

$$\sum_{p<X} \frac{1}{p} = O(\log \log X)$$

程度になってしまうことである. そのため, たとえ膨大な個数の大きな素数に対して上記予想を数値的に検証できたとしても, heuristic から期待される反例の個数の上界がそもそも非常に小さいため, "きっとこの予想は正しい" という確信を得難いのである.

一方, 予想 4.1 や予想 4.2 のような現象は, p 進レギュレーターや (p 進) L 関数の特殊値の mod$p$ 非消滅として解釈すれば, より一般の代数体 (素数 p が馴分岐する "個性的な" 有限次代数体) に対しても類似物を定式化できるはずである. もし, 予想 4.1 や予想 4.2 をそのような形で十分に一般化できれば, 上記 heuristic から期待されるそれらの予想群に対する反例の個数の上界を桁違いに増やすことができるため, 上述のような数値実験に関する心理的な問題を緩和できるであろう. [*5] また, このように手軽な数値実験が可能な予想群は, 代数的整数論の面白さ・不思議さに "初学者が実際に手で触ってみて自発的に気づく" 上でも有意義であると思う.

[*4] 一方, $p = 3$ に対して命題 3.3 を適用すると, $P = 3$ ならば $\iota = 2$ となるが $P = 6$ ならば $\iota = 1$ となる. よって, $P = 6$ を用いることで, 3 の任意の倍数 n に対して, 非特異 n 次平面曲線の局所大域原理の反例の無限族を得る.

[*5] あるいは, もし反例が膨大に見つかれば, それらの規則性を観察するなどして, 予想 4.1 や予想 4.2 の反例の構成に応用できるかもしれない. 従って, 元の予想が正しかろうと正しくなかろうと, それらを一般化する意義はあるはずである. このように, 非常に特殊な場合の考察から生まれた素朴な予想をより一般の場合に洗練していくことで, 元の予想に対する理解を深めていくという研究手法・研究哲学は, 数学の中でも整数論や数論幾何の周辺に顕著な傾向ではないだろうか.

参考文献

[1] N. C. Ankeny, E. Artin, and S. Chowla, *The class-number of real quadratic number fields*, Ann. of Math. (2) **56** (1952), 479–493, DOI 10.2307/1969656. MR0049948

[2] Pierre Barrucand and Harvey Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*, J. Number Theory **2** (1970), 7–21, DOI 10.1016/0022-314X(70)90003-X. MR249398

[3] Pierre Barrucand and Stéphane Louboutin, *Majoration et minoration du nombre de classes d'idéaux des corps réels purs de degré premier*, Bull. London Math. Soc. **25** (1993), no. 6, 533–540, DOI 10.1112/blms/25.6.533 (French, with French summary). MR1245078

[4] T. W. Cusick, *Lower bounds for regulators*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 63–73, DOI 10.1007/BFb0099441. MR756083

[5] Masahiko Fujiwara, *Hasse principle in algebraic equations*, Acta Arith. **22** (1972/73), 267–276, DOI 10.4064/aa-22-3-267-276. MR0319895

[6] Masahiko Fujiwara and Masaki Sudo, *Some forms of odd degree for which the Hasse principle fails*, Pacific J. Math. **67** (1976), no. 1, 161–169. MR0429737

[7] Yoshinosuke Hirakawa and Yosuke Shimizu, *Counterexamples to the local-global principle for non-singular plane curves and a cubic analogue of Ankeny-Artin-Chowla-Mordell conjecture* (2019), available at `arXiv:1912.04600`.

[8] Yoshinosuke Hirakawa, *Primes of the form $X^3 + NY^3$ and a family of non-singular plane curves which violate the local-global princi* (2020), available at `arXiv:2007.11425`.

[9] D. R. Heath-Brown and B. Z. Moroz, *On the representation of primes by cubic polynomials in two variables*, Proc. London Math. Soc. (3) **88** (2004), no. 2, 289–312, DOI 10.1112/S0024611503014497. MR2032509

[10] Debopam Chakraborty and Anupam Saikia, *On a conjecture of Mordell*, Rocky Mountain J. Math. **49** (2019), no. 8, 2545–2556, DOI 10.1216/RMJ-2019-49-8-2545. MR4058336

[11] L. J. Mordell, *On a Pellian equation conjecture. II*, J. London Math. Soc. **36** (1961), 282–288, DOI 10.1112/jlms/s1-36.1.282. MR0126411

[12] Makoto Namba, *Equivalence problem and automorphism groups of certain compact Riemann surfaces*, Tsukuba J. Math. **5** (1981), no. 2, 319–338, DOI 10.21099/tkbjm/1496159409. MR653125

[13] Nguyen Ngoc Dong Quan, *On the Hasse principle for certain quartic hypersurfaces*, Proc. Amer. Math. Soc. **139** (2011), no. 12, 4293–4305, DOI 10.1090/S0002-9939-2011-10936-5. MR2823075

[14] Nguyen Ngoc Dong Quan, *The Hasse principle for certain hyperelliptic curves and forms*, Q. J. Math. **64** (2013), no. 1, 253–268, DOI 10.1093/qmath/har041. MR3032098

[15] Dong Quan Ngoc Nguyen, *Certain forms violate the Hasse principle*, Tokyo J. Math. **40** (2017), no. 1, 277–299, DOI 10.3836/tjm/1502179228. MR3689991

[16] Carl Pomerance, *Remarks on the Pólya-Vinogradov inequality*, Integers **11** (2011), no. 4, 531–542, DOI 10.1515/integ.2011.039. MR2988079

[17] Bjorn Poonen, *An explicit algebraic family of genus-one curves violating the Hasse principle*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 263–274 (English, with English and French summaries). 21st Journées Arithmétiques (Rome, 2001). MR1838086

[18] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216

[19] Ernst S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362 (1 plate), DOI 10.1007/BF02395746. MR0041871

[20] A. J. Van Der Poorten, H. J. J. te Riele, and H. C. Williams, *Corrigenda and addition to: "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100 000 000 000*"*

[Math. Comp. **70** *(2001), no. 235, 1311–1328; MR1709160 (2001j:11125)]*, Math. Comp. **72** (2003), no. 241, 521–523, DOI 10.1090/S0025-5718-02-01527-2. MR1933835