2018 年度藏野研究室卒業論文
「ディオファントス問題について」

明治大学理工学部数学科
佐藤瑞樹
山田莉菜

目次

1 序

整数論とは，整数およびそれから派生する数の体（代数体，局所体など）の性質について研究する数学であり，2000 年以上もの歴史がある．2 つの整数を足し算，引き算，掛け算しても整数になるが，割り算だけは大半が整数にならず，分数になってしまう．しかし，商と余りを用いて表す際には，整数で表すことができる．特に a を b で割ると余りが 0 のとき，b を a の約数といい，また，2 以上の整数 p が $2, \cdots, p-1$ のどれをも約数として持たないとき，p を素数という．この素数 p の性質，特に分布について調べることが整数論の重要なテーマの 1 つである．本論文では，整数論における別の重要なテーマであるディオファントス[1]問題について議論する．

整数論の中でも特に歴史の長いディオファントス問題とは，abc 予想やフェルマー[2]の最終定理などの様々な多変数多項式の有理数解や整数解を求める問題であり，その現代的な解釈を総称したものといえる．ディオファントス問題を攻略するにあたっては，いくつかの方法があるのだが，本論文では，まず第 2 章で，関連の高いディリクレ[3]の定理やリウヴィル[4]の定理から，ディオファントス近似と呼ばれる手法を紹介する．そしてそこから，トゥエ[5]，ジーゲル[6]，ゲルフォント-ダイソン[7]，ロス[8]の近似定理と，改善されていったディオファントス近似定理についても紹介する．第 2 章のトゥエの近似定理に注目して，第 3 章では，その応用として，トゥエ方程式と呼ばれるディオファントス方程式をペル方程式すなわち $x^2 - 2y^2 = 1$ と対応させて紹介する．第 4 章では，ジーゲルの近似定理に注目して，その応用として，彼が証明した単数方程式の美しい結果について紹介する．

ディオファントス近似の中で，次の「フェルマーの最終定理」は非常に有名な定理である．

---

[1] Diophantus of Alexandria(生没年不詳) ローマ帝国時代のエジプトの数学者．「代数学の父」とも呼ばれる．エジプトのアレクサンドリアに住んでいたということ以外は不明．彼の著した 13 巻に及ぶ『算術』が有名である．

[2] Pierre de Fermat(1607-1665) フランスの数学者．「数論の父」とも呼ばれる．

[3] Johann Peter Gustav Lejeune Dirichlet(1805-1859) ドイツの数学者．現代的形式の関数の定義を与えた．

[4] Joseph Liouville(1809-1882) フランスの物理学者，数学者．超越数の最初の例を与えた．

[5] Axel Thue(1863-1922) ノルウェーの数学者．

[6] Carl Ludwig Siegel(1896-1981) ドイツの数学者．

[7] Freeman John Dyson(1923-) イギリスの数学者，物理学者．

[8] Klaus Friedrich Roth(1925-2015) ドイツの数学者．

定理 1.1. n を 3 以上の自然数とする．このとき，

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

を満たす自然数の組 (x, y, z) は存在しない．

1635 年，フェルマーはこの驚くべき定理を予想した．フェルマーをはじめ，数多くの数学者たちがこの問題に挑んできた．そして 1995 年，ワイルズ[9]によって完全に証明された．ワイルズによる証明には非常に高度な数学が駆使されている．そして，フェルマーの最終定理と非常に関連の高いものが下の「abc 予想」である．abc 予想が成り立つとディオファントス方程式に関する様々な結果を直ちに得ることができる．フェルマーの最終定理でさえも abc 予想から簡単に証明できてしまう．

予想 1.2.

$$\mathbf{abc} = \left\{ (a,b,c) \text{ は整数} \;\middle|\; \begin{array}{c} \gcd(a,b,c) = 1 \\ 0 < a < b < c \\ a + b = c \end{array} \right\}$$

とおく．このとき，任意の実数 $\kappa > 1$ に対して，

$$\mathbf{abc}[\kappa] = \left\{ (a,b,c) \in \mathbf{abc} \;\middle|\; c \geq (\mathrm{rad}(\mathbf{abc}))^{\kappa} \right\}$$

は有限集合であろう．

1985 年にオステルレ[10]とマッサー[11]によって提起された abc 予想は 2012 年に望月新一[12]教授が証明を発表し，非常に有名になった．しかし，その論文は専門家にとっても難解であり，まだ評価は確定していない状態である．この予想は第 2 章で紹介するロスの近似定理を強めたものであり，「ABC 定理」の整数における似類である．第 5 章では，この予想が成り立つと仮定して，ビール予想またはタイデマン-ザギエ予想，カタラン予想への応用を試みる．また，最後に abc 予想の精度を高めた，「強い abc 予想」についても述べる．

本論文は，山崎隆雄「初等整数論 ―数論幾何への誘い―」[2]，安福悠「発見・予想を積み重ねる―それが整数論」[1] の一部を自身の言葉でまとめたものである．

---

[9] Andrew John Wiles(1953-) イギリスの数学者．オックスフォード大学教授．

[10] Joseph Oesterle(1954-) フランスの数学者．

[11] David William Masser(1948-) ロンドンの数学者．

[12] 望月新一 (1969-) 日本の数学者．京都大学数理解析研究所教授．専門は数論幾何学，遠アーベル幾何学．

2　ディオファントス近似

一般的にどんな実数に対しても，より長い小数展開を考えると，より誤差の小さい近似をするような有理数が存在する．しかし，その精度に注目すると，約分のできる分数はその分だけ近似分数の分母の数が下がるため，精度にズレが生じてしまう．

これから紹介する定理は，実数の有理数による近似について与えられた結果である．

2.1　ディリクレの近似定理

定理 2.1. α を有理数でない実数とする．このとき

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \tag{2.1}$$

を満たす既約分数 $\frac{p}{q}$ は無限個存在する．

証明. 背理法を用いて証明をしてゆく．(2.1) を満たす既約分数 $\frac{p}{q}$ は有限個しかないと仮定して，それらを

$$\frac{p_1}{q_1}, \cdots, \frac{p_n}{q_n} \tag{2.2}$$

とする．α は有理数ではないので $\left|\alpha - \frac{p_k}{q_k}\right| \neq 0$ $(k = 1, \cdots, n)$ である．そこで，

$$\left|\alpha - \frac{p_k}{q_k}\right| > \frac{1}{q_k N} \quad (k = 1, \cdots, n) \tag{2.3}$$

を満たす自然数 N をとる．つまり，

$$N > \max_{k=1,\cdots,n} \frac{1}{q_k \left|\alpha - \frac{p_k}{q_k}\right|} \tag{2.4}$$

となるように N を選べばよい．

図 2.1　区間 [0,1] の N 等分

次に図 2.1 のように区間 [0,1] を N 等分し，$1 \leq i \leq N+1$ を満たす自然数 i に対して $i\alpha$ の小数部分を b_i とする．このとき，

$$i\alpha = n_i + b_i \quad (n_i\text{は整数}, 0 \leq b_i < 1)$$

となる．ここで，$b_1, \cdots, b_{N+1}$ は無理数であることに注意する．$b_1, \cdots, b_{N+1}$ はそれぞれ区間 $[0,1]$ を N 等分した開区間のいずれかに入るので，鳩の巣論法[13]より，

$$|b_j - b_i| < \frac{1}{N}$$

を満たす $1 \leq i < j \leq N+1$ が存在する．すなわち

$$|(j\alpha - n_j) - (i\alpha - n_i)| = |(j-i)\alpha - (n_j - n_i)| < \frac{1}{N}$$

となることがわかる．この不等式を $j-i$ で割ると

$$\left|\alpha - \frac{n_j - n_i}{j-i}\right| < \frac{1}{(j-i)N}$$

となり，$\frac{n_j-n_i}{j-i}$ の既約分数を $\frac{p}{q}$ とする (ただし，q は自然数とする) と $q \leq j-i$ であるので，従って，

$$\left|\alpha - \frac{n_j - n_i}{j-i}\right| < \frac{1}{(j-i)N} \leq \frac{1}{qN}$$

がわかる．この式と (2.3) に注目すると，(2.2) には $\frac{p}{q}$ が出てこないことがわかる．しかし，$j-i \leq N+1-1 = N$ であるので

$$\left|\alpha - \frac{n_j - n_i}{j-i}\right| < \frac{1}{(j-i)N} \leq \frac{1}{(j-i)^2} \leq \frac{1}{q^2}$$

となる．よって，式 (2.1) を満たす (2.2) 以外の既約分数 $\frac{p}{q}$ が存在するので，背理法の仮定に矛盾する．故に，式 (2.1) を満たす既約分数 $\frac{p}{q}$ は無限個存在する． □

2.2 リウヴィルの近似定理

ディリクレの定理は近似分数が無限個であるという結果であったが，実は近似の精度を高めることによって，近似分数が有限個になる．これがディオファントス近似の重要な問題であり，次の定理はディリクレよりも前に知られていた結果である．

[13]鳩の巣論法とは，「$N+1$ 羽の鳩を N 個の巣に入れるとき，$N+1 > N$ であるので，少なくとも 1 個の巣には 1 羽より多い鳩が中に入る」というものである．

定理 2.2. α を有理数でない実数で，d 次の整数係数多項式

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

の根とする．このとき，$\rho > d$ ならば

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\rho} \tag{2.5}$$

を満たす既約分数 $\frac{p}{q}$ は有限個である．

証明. $d = 1$ ならば $f(\alpha) = 0$ は無理数の解を持たない．よって，$d \geq 2$ であることに注意する．$f(x)$ を α の $\mathbb{Q}$ 上の最小多項式に取り換えることにより，$f(x)$ は $\mathbb{Q}$ 上既約であるとしてよい．$f(x)$ は d 次の整数係数多項式であるので，その 1 階微分は $d-1$ 次多項式，2 階微分は $d-2$ 次多項式であり，d 階微分は 0 次多項式，つまり定数となる．当然 $d+1$ 階微分以降は 0 となる．よって，$x = \alpha$ のまわりでの $f(x)$ のテイラー展開は

$$f(x) = f(\alpha) + f'(\alpha)(x-\alpha) + \frac{f''(\alpha)}{2!}(x-\alpha)^2 + \cdots + \frac{f^{(d)}(\alpha)}{d!}(x-\alpha)^d$$

となる．ここで，$f(\alpha) = 0$ に注意する．これに絶対値をつけた式は，三角不等式によって

$$\begin{aligned} |f(x)| &\leq |f'(\alpha)(x-\alpha)| + \left| \frac{f''(\alpha)}{2!}(x-\alpha)^2 \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!}(x-\alpha)^d \right| \\ &= |f'(\alpha)|\,|x-\alpha| + \left| \frac{f''(\alpha)}{2!} \right| |x-\alpha|^2 + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right| |x-\alpha|^d \end{aligned} \tag{2.6}$$

となる．

以下，$\frac{p}{q}$ は既約分数で，

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\rho} \leq 1$$

と仮定する．ここで，

$$\left| \frac{p}{q} - \alpha \right|^i \leq \left| \frac{p}{q} - \alpha \right| \quad (i \text{ は自然数})$$

となることに注意する．(2.6) の x に $\frac{p}{q}$ を代入すると

$$\begin{aligned} \left| f\left(\frac{p}{q}\right) \right| &\leq |f'(\alpha)| \left| \frac{p}{q} - \alpha \right| + \left| \frac{f''(\alpha)}{2!} \right| \left| \frac{p}{q} - \alpha \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right| \left| \frac{p}{q} - \alpha \right| \\ &= \left(|f'(\alpha)| + \left| \frac{f''(\alpha)}{2!} \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right| \right) \left| \frac{p}{q} - \alpha \right| \end{aligned}$$

$$< \left(|f'(\alpha)| + \left| \frac{f''(\alpha)}{2!} \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right| \right) \frac{1}{q^\rho} \tag{2.7}$$

となる．$f(x)$ は整数係数多項式であるので

$$\begin{aligned} f\left(\frac{p}{q}\right) &= a_d \left(\frac{p}{q}\right)^d + a_{d-1} \left(\frac{p}{q}\right)^{d-1} + \cdots + a_1 \frac{p}{q} + a_0 \\ &= \frac{a_d p^d + a_{d-1} p^{d-1} q + \cdots + a_1 p q^{d-1} + a_0 q^d}{q^d} \end{aligned} \tag{2.8}$$

は有理数である．$f(x)$ は $\mathbb{Q}$ 上既約であるので，$f(\frac{p}{q}) \neq 0$ となる．よって，

$$\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^d} \tag{2.9}$$

がわかる．これを (2.7) と合わせて

$$\frac{1}{q^d} \leq \left| f\left(\frac{p}{q}\right) \right| \leq \frac{|f'(\alpha)| + \left| \frac{f''(\alpha)}{2!} \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right|}{q^\rho}$$

となる．両辺に q^ρ を掛けて

$$q^{\rho - d} \leq |f'(\alpha)| + \left| \frac{f''(\alpha)}{2!} \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right|$$

となり，よって

$$q \leq \left(|f'(\alpha)| + \left| \frac{f''(\alpha)}{2!} \right| + \cdots + \left| \frac{f^{(d)}(\alpha)}{d!} \right| \right)^{\frac{1}{\rho - d}} \tag{2.10}$$

となる．q を 1 つ固定し，$\frac{i}{q} \leq \alpha < \frac{i+1}{q}$ とすると，$p \neq i, i+1$ のとき

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q} > \frac{1}{q^\rho}$$

となり (2.5) を満たさない．つまり，q を 1 つ固定した場合，(2.5) を満たす $\frac{p}{q}$ は高々 2 個になる．(2.10) により q の可能性は有限であり，1 つの q に対して高々 2 個の p しか (2.5) を満たさないので，(2.5) を満たす既約分数 $\frac{p}{q}$ は有限個である． □

2.3 改善された近似定理

ディオファントス方程式についての結果を得るためには，「もう少し緩い近似精度でも近似分数が有限個しかない」という主張が必要である．ディオファントス近似に関して多くの数学者たちがその主張を導き出すために挑み，結果を改善していった．次の定理では，トゥエ，ジーゲル，ゲルフォント-ダイソン，ロスの近似定理を紹介する．

定理 2.3. α を有理数でない実数で，d 次の整数係数多項式

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

の根とする．このとき，ρ を次の (i)〜(iv) のいずれかの条件を満たすものとして 1 つ固定すると，

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\rho} \tag{2.11}$$

を満たす既約分数 $\frac{p}{q}$ は有限個である．

(i) (トゥエ)　$\rho > \frac{d}{2} + 1$
(ii) (ジーゲル)　$\rho > 2\sqrt{d}$
(iii) (ゲルフォント-ダイソン)　$\rho > \sqrt{2d}$
(iv) (ロス)　$\rho > 2$

定理 2.3 は証明が非常に難しいので，ここで証明することはできない．

d が十分大きいならば $d > \frac{d}{2} + 1 > 2\sqrt{d} > \sqrt{2d} > 2$ となり，ロスの定理が (2.11) の最も近似精度が緩いものになっている．また，ディリクレの定理では $\frac{1}{q^2}$ 未満に近似する $\frac{p}{q}$ が無限個であり，ロスの定理では $\rho > 2$ のときに有限個であると主張しているので，2 がちょうど境目になっていることがわかる．つまり，ロスの定理が最良なものであることがわかる．

この定理はディオファントス方程式をはじめ，多くのものに応用することができる．以下の章では，トゥエの定理からディオファントス方程式へ，ジーゲルの定理から単数方程式への応用について紹介する．

3　ディオファントス方程式

この章では，前章で述べたトゥエの近似定理からディオファントス方程式への応用について紹介する．

3.1　ペル方程式

まずは，ペル方程式という有名なディオファントス方程式について考える．

定理 3.1. ペル方程式 $x^2 - 2y^2 = 1$ の自然数解 (x, y) は，無限個存在する．

証明. a, b を自然数とし，$a + b\sqrt{2}$ のノルムを $N(a + b\sqrt{2}) = a^2 - 2b^2$ と定義する．

このとき，自然数 a, b, c, d に対して

$$\begin{aligned} N\left((a+b\sqrt{2})(c+d\sqrt{2})\right) &= N\left((ac+2bd)+(ad+bc)\sqrt{2}\right) \\ &= (ac+2bd)^2 - 2(ad+bc)^2 \\ &= a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2 \\ &= (a^2-2b^2)(c^2-2d^2) \\ &= N(a+b\sqrt{2})N(c+d\sqrt{2}) \end{aligned}$$

が成り立つ．よって，

$$N\left((3+2\sqrt{2})^n\right) = N(3+2\sqrt{2})^n = 1^n = 1$$

となる．$(3+2\sqrt{2})^n = x_n + y_n\sqrt{2}$ とおくと，$x_1 < x_2 < \cdots$ であるので，

$$\{(x_n, y_n) | n = 1, 2, \cdots\}$$

はペル方程式の無限個の解を与えている． □

3.2 トゥエ方程式

ペル方程式では 2 次のディオファントス方程式について考えてきたが，次数を上げた問題について考えていこう．

定理 3.2. d, m を自然数とし，d は 3 以上，m は自然数の d 乗ではないとする．このとき

$$x^d - my^d = 1 \tag{3.1}$$

の整数解 (x, y) の個数は高々有限個である．

証明. 整数 x, y が (3.1) を満たすとする．$y \neq 0$ とする．このとき，x と y は互いに素であることに注意する．(3.1) の両辺を y^d で割ると

$$\left(\frac{x}{y}\right)^d - m = \frac{1}{y^d} \tag{3.2}$$

となる．$X^d - m = 0$ の複素数解は

$$\left\{ \sqrt[d]{m} \cdot e^{\frac{2\pi l i}{d}} \mid l = 0, \cdots, d-1 \right\}$$

であるので，

$$X^d - m = (X - \sqrt[d]{m})(X - \sqrt[d]{m} \cdot e^{\frac{2\pi i}{d}})(X - \sqrt[d]{m} \cdot e^{\frac{4\pi i}{d}}) \cdots (X - \sqrt[d]{m} \cdot e^{\frac{2(d-1)\pi i}{d}}) \tag{3.3}$$

となる．この式の X に $\frac{x}{y}$ を代入し，(3.2) に絶対値を付けると，

$$\left|\frac{x}{y}-\sqrt[d]{m}\right|\left|\frac{x}{y}-\sqrt[d]{m}\cdot e^{\frac{2\pi i}{d}}\right|\left|\frac{x}{y}-\sqrt[d]{m}\cdot e^{\frac{4\pi i}{d}}\right|\cdots\left|\frac{x}{y}-\sqrt[d]{m}\cdot e^{\frac{2(d-1)\pi i}{d}}\right|=\left|\frac{1}{y^d}\right| \tag{3.4}$$

となる．ここで次の主張を証明する．

主張 3.3. d と m に依存する定数 C が存在して，(3.1) を満たす任意の整数解 (x,y) (ただし，$y\neq 0$) に対して

$$\left|\frac{x}{y}-\varepsilon\sqrt[d]{m}\right|\leq\left|\frac{C}{y^d}\right| \tag{3.5}$$

が成り立つ．ただし，d が奇数のときは $\varepsilon=1$，d が偶数で x と y が同符号のときは $\varepsilon=1$，d が偶数で x と y が異符号のときは $\varepsilon=-1$ と定める．

証明. d が奇数の場合は $l=1,\cdots,d-1$ とするとき，$\sqrt[d]{m}\cdot e^{\frac{2\pi li}{d}}$ は実数ではない．そこで，これらの複素数の虚部のうち最小絶対値のものを C' とすると，$\frac{x}{y}$ は実数なので

$$\left|\frac{x}{y}-\sqrt[d]{m}\cdot e^{\frac{2\pi li}{d}}\right|\geq C'\quad(l=1,\cdots,d-1)$$

となる．よって (3.4) と合わせて，

$$\left|\frac{x}{y}-\sqrt[d]{m}\right|\leq\left|\frac{1}{y^d}\right|\times\frac{1}{(C')^{d-1}}$$

となるので，$C=\frac{1}{(C')^{d-1}}$ とおけばよい．

d が偶数の場合を考えよう．$l\neq\frac{d}{2}$ のときは，$\sqrt[d]{m}\cdot e^{\frac{2\pi li}{d}}$ は実数ではないので，奇数の場合と同様にこれらの複素数の虚部のうち最小絶対値のものを C' とすると，

$$\left|\frac{x}{y}-\sqrt[d]{m}\cdot e^{\frac{2\pi li}{d}}\right|\geq C'\quad\left(l=1,\cdots,\frac{d}{2}-1,\frac{d}{2}+1,\cdots,d-1\right)$$

となる．$l=\frac{d}{2}$ のときは，

$$\sqrt[d]{m}\cdot e^{\frac{2\pi\frac{d}{2}i}{d}}=\sqrt[d]{m}\cdot e^{\pi i}=-\sqrt[d]{m}$$

となり，実数になる．しかし，x と y が同符号のとき $\frac{x}{y}$ と $-\sqrt[d]{m}$ との距離は少なくとも $\sqrt[d]{m}$ あるので，

$$\left|\frac{x}{y}-\sqrt[d]{m}\right|\leq\left|\frac{1}{y^d}\right|\times\frac{1}{(C')^{d-2}\cdot\sqrt[d]{m}}$$

となる．x と y が異符号のときは $\frac{x}{y}$ と $\sqrt[d]{m}$ との距離が少なくとも $\sqrt[d]{m}$ あるので，

$$\left|\frac{x}{y} - (-\sqrt[d]{m})\right| \leq \left|\frac{1}{y^d}\right| \times \frac{1}{(C')^{d-2} \cdot \sqrt[d]{m}}$$

となる．よって，d が偶数の場合は，

$$C = \frac{1}{(C')^{d-2}\sqrt[d]{m}}$$

とおけばよい． □

定理 3.2 の証明に戻る．ここで，$d \geq 3$ であるので，$\frac{d}{2} + 1 < d$ となる．$\frac{d}{2} + 1 < \rho < d$ を満たすような ρ をとる．C は主張 3.3 で選んだ数とする．このとき，(3.1) の解 (x, y) に対して，

$$\left|\frac{C}{y^d}\right| < \frac{1}{|y|^\rho}$$

のときは，(3.5) と合わせて，

$$\left|\frac{x}{y} - \varepsilon\sqrt[d]{m}\right| < \frac{1}{|y|^\rho}$$

となる．定理 2.3(トゥエの定理) より，これを満たす $\frac{x}{y}$ は有限個であることがわかる．また，

$$\left|\frac{C}{y^d}\right| \geq \frac{1}{|y|^\rho}$$

のときは，$|y|^d$ を掛けると，

$$|C| \geq |y|^{d-\rho}$$

となり，y は有限個になる．y を 1 つ固定すると，(3.1) を満たす整数 x は高々 2 個であるので，解 (x, y) は有限個である．これによって，(3.1) を満たす整数解が有限個であることがわかった． □

4　単数方程式

この章では，第 2 章で述べたジーゲルの近似定理から単数方程式への応用について紹介する．

素数の有限集合 $S = \{p_1, p_2, \cdots, p_k\}$ を固定したとき，自然数の集合

$$\{p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_k^{n_k} \mid n_1, \cdots, n_k \geq 0\}$$

を S 単数という．これに対して，ジーゲルは次の定理を証明した．

定理 4.1. S を素数の有限集合とするとき，$\gcd(a,b,c)=1$ で

$$a+b=c$$

を満たす S 単数の組 (a,b,c) は高々有限個である．

証明. 背理法によって示す．$S=\{p_1,p_2,\cdots,p_k\}$ とおき，単数方程式の解が無限個あると仮定する．単数方程式の解 (a,b,c) は，2 つずつが互いに素であることに注意する．$c-b=a$ の両辺を a で割ると，

$$\frac{c}{a}-\frac{b}{a}=1 \tag{4.1}$$

となる．$\frac{c}{a}$ と $\frac{b}{a}$ は既約分数であり，$\frac{c}{a}$ と $\frac{b}{a}$ は

$$R_S^*=\{p_1^{n_1}\times p_2^{n_2}\times\cdots\times p_k^{n_k}\mid n_1,\cdots,n_k\text{は整数}\}$$

の元となる．ここで，d は $d>4(k+1)^2$ を満たす自然数とする．自然数の部分集合 T を，

$$T=\{p_1^{n_1}\times p_2^{n_2}\times\cdots\times p_k^{n_k}\mid 0\le n_i<d\ (1\le i\le k)\}$$

と定義する．さらに，

$$A:=\left\{\left(\frac{c}{a},\frac{b}{a}\right)\;\middle|\;\begin{array}{c}a,b,c\text{ は }S\text{ 単数}\\ a+b=c\\ a,b,c\text{ の 2 つずつは互いに素}\end{array}\right\}$$

と定める．A の元 $\left(\frac{c}{a},\frac{b}{a}\right)$ に対して，$\sqrt[d]{\frac{\left(\frac{c}{a}\right)}{\alpha}}$ と $\sqrt[d]{\frac{\left(\frac{b}{a}\right)}{\beta}}$ が共に R_S^* の元となるような，T の元 α,β が一意的に存在する．このことから，

$$\varphi\left(\left(\frac{c}{a},\frac{b}{a}\right)\right)=(\alpha,\beta)$$

によって写像

$$\varphi:A\to T^2$$

を構成することができる．仮定より $\#A=\infty$ であり，$\#T<\infty$ である．よって，$\#\varphi^{-1}((\alpha,\beta))=\infty$ となる α,β を T から選ぶことができる．以下，$\#\varphi^{-1}((\alpha,\beta))=\infty$ と仮定する．(γ,δ) を $\varphi^{-1}((\alpha,\beta))$ の元としよう．このとき，$X=\sqrt[d]{\frac{\gamma}{\alpha}}$，$Y=\sqrt[d]{\frac{\delta}{\beta}}$ とおくと，X,Y は R_S^* の元であり，

$$\alpha X^d-\beta Y^d=1 \tag{4.2}$$

を満たす．(4.2) の両辺を αY^d で割ると

$$\left(\frac{X}{Y}\right)^d - \frac{\beta}{\alpha} = \frac{1}{\alpha Y^d} \tag{4.3}$$

となる．ここで，定理 3.2 の証明と同様に，$Z^d - \frac{\beta}{\alpha} = 0$ の複素数解は

$$\left\{ \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi l i}{d}} \middle| \, l = 0, \cdots, d-1 \right\}$$

となる．これによって，

$$Z^d - \frac{\beta}{\alpha} = (Z - \sqrt[d]{\frac{\beta}{\alpha}})(Z - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi i}{d}})(Z - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{4\pi i}{d}}) \cdots (Z - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2(d-1)\pi i}{d}}) \tag{4.4}$$

となる．この式の Z に $\frac{X}{Y}$ を代入し，(4.3) に絶対値を付けると，

$$\left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}}\right| \left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi i}{d}}\right| \left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{4\pi i}{d}}\right| \cdots \left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2(d-1)\pi i}{d}}\right| = \left|\frac{1}{\alpha Y^d}\right| \tag{4.5}$$

となる．ここで次の主張を証明する．

主張 4.2. d, α, β のみに依存する定数 C が存在して，(4.2) を満たす正の有理数解 (X, Y) に対して

$$\left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}}\right| \leq \left|\frac{C}{Y^d}\right| \tag{4.6}$$

が成り立つ．

証明． d が奇数の場合は，$l = 1, \cdots, d-1$ のとき，$\sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi l i}{d}}$ は実数ではない．そこで，これらの複素数の虚部のうち最小絶対値のものを C' とすると，$\frac{X}{Y}$ は実数なので

$$\left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi l i}{d}}\right| \geq C' \quad (k = 1, \cdots, d-1)$$

となる．よって (4.5) と合わせて，

$$\left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}}\right| \leq \left|\frac{1}{\alpha Y^d}\right| \times \frac{1}{(C')^{d-1}}$$

となるので，$C = \frac{1}{\alpha (C')^{d-1}}$ とおけばよい．

d は偶数とする．$l \neq \frac{d}{2}$ のときは $\sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi l i}{d}}$ は実数ではないので，これらの複素数の虚部のうち最小絶対値のものを C' とすると，

$$\left| \frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi l i}{d}} \right| \geq C' \quad (l = 1, \cdots, \frac{d}{2} - 1, \frac{d}{2} + 1, \cdots, d - 1)$$

となる．$l = \frac{d}{2}$ のときは，

$$\sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\frac{2\pi \frac{d}{2} i}{d}} = \sqrt[d]{\frac{\beta}{\alpha}} \cdot e^{\pi i} = -\sqrt[d]{\frac{\beta}{\alpha}}$$

となり，実数になる．しかし，X と Y は 0 以上であり，$\frac{X}{Y}$ と $-\sqrt[d]{\frac{\beta}{\alpha}}$ との距離は少なくとも $\sqrt[d]{\frac{\beta}{\alpha}}$ ある．よって，

$$\left| \frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \right| \leq \left| \frac{1}{\alpha Y^d} \right| \times \frac{1}{(C')^{d-2} \cdot \sqrt[d]{\frac{\beta}{\alpha}}}$$

となる．よって，$C = \frac{1}{\alpha (C')^{d-2} \cdot \sqrt[d]{\frac{\beta}{\alpha}}}$ とおけばよい． □

ここで，Y は有理数であるので，(4.6) の右辺が 1 より大きくなる場合がある．そのような場合には，通常の絶対値ではなく，p 進絶対値[14]を用いる．また，近似定理は 1 つ 1 つの絶対値ごとに独立して成り立つわけではない．また，高さ関数 H を考える．[15]

これらを導入することによって，定理 2.3 の p 進絶対値版である次の主張 4.3 が成立することが知られている．ここでは，証明は省略する．

主張 4.3. δ が d 次の整数係数多項式の根であり (ただし，δ は有理数ではないとする)，$\rho > 2\sqrt{d}$ とする．このとき，

$$\left| \frac{f}{g} - \delta \right|_p < \frac{1}{H\left(\frac{f}{g}\right)^\rho}$$

を満たす既約分数 $\frac{f}{g}$ は有限個である．

さらに，主張 4.2 の p 進絶対値版である次の主張 4.4 も成立することが知られている．これも証明は省略する．

---

[14] p を素数とする．0 でない有理数は，$p^h \cdot \frac{q}{r}$ (h, q, r は整数, $\gcd(q, p) = \gcd(r, p) = 1$) と書ける．このとき，$p$ 進絶対値を $\left|p^h \cdot \frac{q}{r}\right|_p = p^{-h}$ と定義する．p 進絶対値は，代数体上でも定義できる．

[15] 既約分数 $\frac{q}{r}$ の高さを，$H\left(\frac{q}{r}\right) = \max\{|q|, |r|\}$ と定義する．

主張 4.4. d, α, β のみに依存する定数 C が存在して，(4.2) を満たす正の有理数解 (X, Y) に対して

$$\left| \frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \right|_p \leq \left| \frac{C}{Y^d} \right|_p \tag{4.7}$$

が成り立つ．

これで (4.6) と (4.7) という 2 つの不等式が得られた．このとき，次の主張が証明できる．

主張 4.5. (X, Y) は (4.2) を満たす R_S^* の元のペアとする．このとき，S と d にのみ依存する定数 C'' が存在して，

$$H\left(\frac{X}{Y}\right) \leq C'' \left|Y\right|_v^{k+1} \tag{4.8}$$

を満たす．ただし，$|\ |_v$ は，通常の絶対値 $|\ |$ または $|\ |_{p_1}, \cdots, |\ |_{p_k}$ のどれかである．(ただし，$S = \{p_1, \cdots, p_k\}$ は最初に固定した有限個の素数の集合である．)

証明. (4.3) を移項して，

$$\left(\frac{X}{Y}\right)^d = \frac{\beta}{\alpha} + \frac{1}{\alpha Y^d}$$

とする．ここで，高さ関数 H の性質[16]より

$$H\left(\frac{X}{Y}\right)^d \leq 2H\left(\frac{\beta}{\alpha}\right) H(\alpha) H(Y)^d$$

となる．つまり，

$$H\left(\frac{X}{Y}\right) \leq \sqrt[d]{2H\left(\frac{\beta}{\alpha}\right) H(\alpha)} H(Y)$$

となる．

ここで，$H(Y) \leq |Y|_v^{k+1}$ を満たすような $|\ |_v$ が存在することを示す (ただし，$|\ |_v$ は通常の絶対値または S の元 p による p 進絶対値 $|\ |_p$ である．)．必要なら S の元の番号を付け替えることにより，

$$S = \{p_1, \cdots, p_t, p_{t+1}, \cdots, p_k\}$$

$$Y = \pm \frac{p_1^{a_1} \cdots p_t^{a_t}}{p_{t+1}^{a_{t+1}} \cdots p_k^{a_k}} \quad (a_i \text{は非負整数})$$

[16] $H : \mathbb{Q}^\times \to \mathbb{N},\ \frac{q}{r} \mapsto \max\{|q|, |r|\}$ と定める．ζ, η を $\mathbb{Q}^\times$ の元としたとき (1) $H(\zeta\eta) \leq H(\zeta)H(\eta)$, (2) $H(\zeta^n) = H(\zeta)^n$, (3) $H(\zeta \pm \eta) \leq 2H(\zeta)H(\eta)$, (4) $H\left(\frac{1}{\zeta}\right) = H(\zeta)$ が成り立つ．

とする．すると，

$$|Y|_{p_i} = \begin{cases} p_i^{-a_i} & (i = 1, \cdots, t) \\ p_i^{a_i} & (i = t+1, \cdots, k) \end{cases}$$

が成立する．

$p_1^{a_1} \cdots p_t^{a_t} < p_{t+1}^{a_{t+1}} \cdots p_k^{a_k}$ のとき

$$H(Y) = p_{t+1}^{a_{t+1}} \cdots p_k^{a_k} = |Y|_{p_{t+1}} \cdots |Y|_{p_k}$$

となり，$t+1 \leq i \leq k$ を満たすある i に対して，

$$\sqrt[k+1]{H(Y)} \leq \sqrt[k-t]{H(Y)} \leq |Y|_{p_i}$$

であるので，$H(Y) \leq |Y|_{p_i}^{k+1}$ が成り立つ．

$p_1^{a_1} \cdots p_t^{a_t} \geq p_{t+1}^{a_{t+1}} \cdots p_k^{a_k}$ のとき

$$H(Y) = p_1^{a_1} \cdots p_t^{a_t} = |Y|\,|Y|_{p_{t+1}} \cdots |Y|_{p_k}$$

となり，

$$\sqrt[k+1]{H(Y)} \leq \sqrt[k-(t+1)]{H(Y)} \leq |Y|_v$$

であるので，$H(Y) \leq |Y|_v^{k+1}$ が成り立つ．ただし，$|\ |_v$ は $|\ |, |\ |_{p_{t+1}}, \cdots, |\ |_{p_k}$ のどれかとする．$C'' = \sqrt[d]{2H\left(\frac{\beta}{\alpha}\right) H(\alpha)}$ とおくことにより，(4.9) が成り立ち，主張 4.5 の証明は完了した． □

(4.8) によって，

$$\frac{1}{|Y|_v} \leq \left(\frac{C''}{H\left(\frac{X}{Y}\right)} \right)^{\frac{1}{k+1}}$$

を満たすので，主張 4.2 と主張 4.4 を用いることにより，

$$\left| \frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}} \right|_v \leq \left| \frac{C}{Y^d} \right|_v \leq \frac{C'''}{H\left(\frac{X}{Y}\right)^{\frac{d}{k+1}}} \quad (C''' = C \times (C'')^{\frac{d}{k+1}}) \tag{4.9}$$

となる．ところで，d は $d > 4(k+1)^2$ を満たす自然数であった．すると，

$$\frac{d}{k+1} > 2\sqrt{d}$$

を満たす．ここで，ρ を $\frac{d}{k+1} > \rho > 2\sqrt{d}$ ととると，(4.2) の有限個の解を除いて[17]，

$$\left|\frac{X}{Y} - \sqrt[d]{\frac{\beta}{\alpha}}\right|_v \leq \frac{C'''}{H\left(\frac{X}{Y}\right)^{\frac{d}{k+1}}} < \frac{1}{H\left(\frac{X}{Y}\right)^{\rho}} \tag{4.10}$$

となる．

ここで，$\alpha = \beta$ と $\alpha \neq \beta$ の 2 つの場合に分けて考える．$\frac{X}{Y} = \frac{p}{q}$ とおく．ただし，p, q は自然数で，互いに素とする．

$\alpha = \beta$ のときは，$X > Y > 0$ であるので $H\left(\frac{X}{Y}\right) = p$ である．$|\ |_v$ が通常の絶対値とすると，

$$\left|\frac{p-q}{q}\right| = \left|\frac{p}{q} - 1\right| < \frac{1}{p^{\rho}}$$

となる．$\frac{p}{q} \neq 1$ であるので，左辺は $\frac{1}{q}$ より大きい．これは矛盾である．$|\ |_v$ が p_i 進絶対値 $|\ |_{p_i}$ とすると，

$$\left|\frac{p-q}{q}\right|_{p_i} = \left|\frac{p}{q} - 1\right|_{p_i} < \frac{1}{p^{\rho}}$$

となる．$p_i | q$ のとき，

$$\left|\frac{p-q}{q}\right|_{p_i} > 1$$

となり矛盾である．$p_i | p$ のとき，

$$\left|\frac{p-q}{q}\right|_{p_i} = 1$$

となり矛盾である．$p_i \nmid p$ かつ $p_i \nmid q$ のとき，$p - q = p_i^a b$，$(p_i, b) = 1$ とおくと，

$$\left|\frac{p-q}{q}\right|_{p_i} = \frac{1}{p_i^a} < \frac{1}{p^{\rho}}$$

となり，$p^{\rho} < p_i^a < p$ であるので，$\rho > 2\sqrt{d}$ に矛盾する．

$\alpha \neq \beta$ のときは，定義により $\sqrt[d]{\frac{\beta}{\alpha}}$ は有理数でない．

$$H\left(\frac{X}{Y}\right) \geq q$$

であり，

$$\frac{1}{H\left(\frac{X}{Y}\right)^{\rho}} < \frac{1}{q^{\rho}}$$

[17] $H\left(\frac{X}{Y}\right)^{\frac{d}{k+1} - \rho} > C'''$ が成立するように，(4.2) の有限個の解を除く必要がある．

となるので，ジーゲルの近似定理が適用できる．よって，$\frac{X}{Y}$ は有限個であり，(4.10) の際に除いた有限個の (X, Y) を考慮しても，(4.2) の解は有限個とわかる．しかし，(4.2) の R_S^* 内での解が無限個であるので，矛盾が生じる．故に，定理 4.1 の証明は完了した． □

5 ABC 定理と abc 予想

5.1 ABC 定理

以下，K は標数 0 の体とし，0 でない K の元全体の集合を

$$K^\times = \{a \in K \mid a \neq 0\}$$

と書く．

定義 5.1. $n \in \mathbb{Z}_{\geq 0}, a_0, \ldots, a_n \in K$ に対して，

$$A(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0$$

の形に表されるものを多項式といい，多項式全体の集合を

$$K[t] = \{a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \mid n \in \mathbb{Z}_{\geq 0}, a_0, \ldots, a_n \in K\}$$

と書く．零でない多項式 $A(t) \in K[t]$ に対し，$a_n \neq 0$ となる最大の n を考えることができる．このとき n は $A(t)$ の次数といい，$n = \deg A(t)$, $a_n = \epsilon(A(t))$ と表す．

定義 5.2. $I \subset K[t]$ で次の条件を満たすものを $K[t]$ のイデアルという．

(i) $0 \in I$
(ii) $A, B \in I$ のとき，$A + B \in I$
(iii) $A \in I$, $X \in K[t]$ のとき，$AX \in I$

また，$(A) = \{AX \mid X \in K[t]\}$ と書く．

上の (A) は $K[t]$ のイデアルである．$K[t]$ のイデアルは必ず (A) の形をしている．

命題 5.3. 定数でない多項式 $P \in K[t]$ に対し，次の条件は同値である．

(i) $A, B \in K[t]$, $AB \in (P)$ ならば $A \in (P)$ または $B \in (P)$ である．すなわち，P が AB の約数ならば P は A か B の約数である．

(ii) $C \in K[t]$, $P \in (C)$ ならば $(C) = (P)$ または $(C) = (1)$ である. すなわち, P の約数は単数と P の単数倍だけである.

証明. まず (i) を仮定する. $P \in (C)$ となる $C \in K[t]$ をとる. すると, $P = CD$ となる $D \in K[t]$ が存在する. $CD \in (P)$ なので, (i) より $C \in (P)$ または $D \in (P)$ である. 前者の場合, 元の仮定 $P \in (C)$ と合わせて $(C) = (P)$ となる. 後者の場合, ある $E \in K[t]$ により $D = EP$ と書ける. よって, $P = CD = CEP$ から $CE = 1$ がわかる. 従って $(C) = (1)$ となり, (ii) が従う.

次に (ii) を仮定する. $A, B \in K[t]$ が $AB \in (P)$ と $A \notin (P)$ を満たすと仮定して $B \in (P)$ を示す. ここで, $(P, A) = (C)$ となる $C \in K[t]$ が存在する. 一方 $P \in (P, A) = (C)$ より, (ii) を利用して $(C) = (P)$ または $(C) = (1)$ となる. $(C) = (P)$ のとき, $A \in (P, A) = (C) = (P)$ となり, 仮定である $A \notin (P)$ に反する. 従って $(P, A) = 1$ であり, $PX + AY = 1$ となる $X, Y \in K[t]$ が存在する. 仮定より, $AB \in (P)$ なので $B = BPX + BAY \in (P)$ である. 従って, $A, B \in K[t]$ が $AB \in (P)$ と $A \notin (P)$ を満たすとき $B \in (P)$ となったので, (i) が従うことがわかる.

以上より, 二つの条件は同値である. □

定義 5.4. $P \in K[t]$ を定数でない多項式とする. 命題 5.3 の同値な条件が成り立つとき, P を**既約多項式**という. モニックな既約多項式を**素式**と呼ぶ.

定義 5.5. 定数でない多項式 $A \in K[t]$ に対し, A の素因子すべての積を $\mathrm{rad}A$ と書く. すなわち, 相異なる素式 $P_1, \ldots, P_r$ と $e_1, \ldots, e_r \in \mathbb{Z}_{>0}$ について $A = \epsilon(A)P_1^{e_1} \cdots P_r^{e_r}$ のとき $\mathrm{rad}A = P_1 \cdots P_r$ である.

定理 5.6. **(ABC 定理)** $A, B, C \in K[t]$ を, 少なくとも一つは定数ではなく, どの二つも互いに素な多項式で, さらに $A + B = C$ を満たすものとする. [18] このとき, 次が成り立つ.

$$\max(\deg A, \deg B, \deg C) < \deg \mathrm{rad}(ABC).$$

ABC 定理の証明には多項式の微分を用いる. そのため, 証明に移る前に微分の基本性質をまとめておく.

[18] このとき, A, B, C はすべて 0 ではないことに注意する. よって, $\deg A$, $\deg B$, $\deg C$ を考えることができる.

補題 5.7. (微分の性質) $A = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in K[t]$ の微分 $A' \in K[t]$ を

$$A' = na_n t^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + 2a_2 t + a_1$$

と定義する. $A, B \in K[t]$ を 0 でない多項式, $a, b \in K$, $e \in \mathbb{Z}_{>0}$ とすると, 次が成り立つ.

(i) $A' = 0$ と A が定数であることは同値である.
(ii) $(aA + bB)' = aA' + bB'$.
(iii) A が定数でなければ $\deg A' = \deg A - 1$.
(iv) $(AB)' = A'B + AB'$.
(v) $B \in (A^e)$ ならば $B' \in (A^{e-1})$.
(vi) $AB' = BA'$ であることと, $A = cB$ となる数 $c \in K^\times$ が存在することは同値である.

証明. (i)-(iii) は自明.
まず (iv) を示す.

$$A(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$
$$B(t) = b_m t^m + b_{m-1}t^{m-1} + \cdots + b_1 t + b_0$$

とすると,

$$\begin{aligned} AB = {} & a_n b_m t^{n+m} + (a_n b_{m-1} + a_{n-1}b_m)t^{n+m-1} + \cdots \\ & + (a_2 b_0 + a_1 b_1 + a_0 b_2)t^2 + (a_1 b_0 + a_0 b_1)t + a_0 b_0 \end{aligned}$$

となる. これを微分すると,

$$\begin{aligned} (AB)' = {} & (m+n)a_n b_m t^{n+m-1} + (n+m-1)(a_n b_{m-1} + a_{n-1}b_m)t^{n+m-2} + \cdots \\ & + 2(a_2 b_0 + a_1 b_1 + a_0 b_2)t + (a_1 b_0 + a_0 b_1) \end{aligned}$$

となる. 一方,

$$\begin{aligned} A'B = {} & na_n b_m t^{n+m-1} + ((n-1)a_{n-1}b_m + na_n b_{m-1})t^{n+m-2} + \cdots \\ & + (a_1 b_1 + 2a_2 b_0)t + a_1 b_0 \end{aligned}$$

$$\begin{aligned} AB' = {} & ma_n b_m t^{n+m-1} + ((m-1)a_n b_{m-1} + ma_{n-1}b_m)t^{n+m-2} + \cdots \\ & + (a_1 b_1 + 2a_0 b_2)t + a_0 b_1 \end{aligned}$$

となる. よって,

$$\begin{aligned} A'B + AB' &= (m+n)a_n b_m t^{n+m-1} + (n+m-1)(a_n b_{m-1} + a_{n-1} b_m) t^{n+m-2} + \cdots \\ &\quad + 2(a_2 b_0 + a_1 b_1 + a_0 b_2)t + (a_1 b_0 + a_0 b_1) \\ &= (AB)' \end{aligned}$$

がわかる. 従って, $(AB)' = A'B + AB'$ が成立する.
(v) を示す. $B = A^e C$, $C \in K[t]$ とすると, (iv) より

$$B' = (A^e C)' = A^e C' + eA^{e-1}A'C = A^{e-1}(AC' + eA'C)$$

となる. よって, $B' \in (A^{e-1})$ が従う.
次に, (vi) を示す. $A = cB$ と書ければ $AB' = BA'$ は明らかに成立する. 次に, $AB' = BA'$ を仮定する. ここで, $\epsilon(AB') = m\epsilon(A)\epsilon(B)$, $\epsilon(BA') = n\epsilon(A)\epsilon(B)$ より, $\deg A = \deg B$ がわかる. このことから, $B = cA + D$ と書ける ($c \in K^\times, \deg D < \deg A$). このとき, $BA' = cAA' + DA'$, $AB' = AcA' + AD'$ なので, $AB' = BA'$ より $AD' = DA'$ がわかる. また, $\deg D < \deg A$ なので $D = 0$ となる. よって, $B = cA$ となることがわかる.

以上のことを利用して ABC 定理を示してゆく.

定理 5.6. の証明

$D = AB' - BA'$ とする. 微分の性質 (ii) を用いると, $A + B = C$ より $A' + B' = C'$ がいえる. よって,

$$D = AB' - BA' = A(C' - A') - (C - A)A' = AC' - CA'$$

となる. 同様に,

$$D = AB' - BA' = (C - B)B' - B(C' - B') = CB' - BC'$$

となる. ここで, A, B, C は少なくとも一つは定数ではなくどの二つも互いに素なので, $A \neq 0$, $B \neq 0$, $C \neq 0$ となる. これを用いると, 微分の性質 (vi) より

$$D = AC' - CA' = CB' - BC' \neq 0$$

がわかる. また, $A + B = C$ なので, A, B, C の中の二つ以上が定数になることはないことに注意する.

A, B は共に定数でないと仮定する. 微分の性質 (iii) を用いると, $\deg B' = \deg B - 1$ より $\deg A + \deg B' = \deg A + \deg B - 1$ がいえる. ここで,

$$\deg(AB') = \deg(AB) - 1$$

$$\deg(BA') = \deg(AB) - 1$$

を使う. これより,

$$\begin{aligned}\deg(AB' - BA') &\leq \max(\deg(AB'), \deg(BA')) \\ &= \deg(AB) - 1\end{aligned}$$

となる. 以上より,

$$\deg D \leq \deg(AB) - 1$$

がいえる. この式は, A, B の片方が定数の場合も成立することに注意する. 従って, 両辺に $\deg C$ を足して

$$\deg C + \deg D < \deg(ABC)$$

が得られる. $D = AC' - CA' = CB' - BC'$ であるので,

$$\deg A + \deg D < \deg(ABC)$$

$$\deg B + \deg D < \deg(ABC)$$

が得られる. 以上より,

$$\max(\deg A, \deg B, \deg C) + \deg D < \deg(ABC) \tag{5.1}$$

がいえる.

次に, $A_1 = \frac{A}{\mathrm{rad}A}, B_1 = \frac{B}{\mathrm{rad}B}, C_1 = \frac{C}{\mathrm{rad}C}$ とする. ここで, 相異なる素式 $P_1, \ldots, P_r$ と $e_1, \ldots, e_r \in \mathbb{Z}_{>0}$ を用いて, A を

$$A = \epsilon(A) P_1^{e_1} \cdots P_r^{e_r}$$

と素式分解する. すると,

$$A_1 = \frac{A}{\mathrm{rad}A} = \epsilon(A) P_1^{e_1 - 1} \cdots P_r^{e_r - 1}$$

となる. (A が定数の場合は $\mathrm{rad}A = 1$, $A = A_1$ と考える.)

e_i の定義より $A \in (P_i{}^{e_i}) \subset (P_i{}^{e_i - 1})$ となるので, 微分の性質 (v) より $A' \in (P_i{}^{e_i - 1})$ がいえる. 以上より $D = AB' - BA'$ から, 各 $i = 1, \ldots, r$ に対して $D \in (P_i{}^{e_i - 1})$ がわかる. 従って, $D \in (A_1)$ がいえ, 同様にして $D \in (B_1)$, $D \in (C_1)$ もいえる. 加えて A_1, B_1, C_1 はどの二つも互いに素なので, $D \in (A_1 B_1 C_1)$ がわかる. また, $\mathrm{rad}(ABC) = \mathrm{rad}(A)\mathrm{rad}(B)\mathrm{rad}(C)$ であるので,

$$\mathrm{rad}(ABC) A_1 B_1 C_1 = ABC$$

となる. よって,

$$D \times \mathrm{rad}(ABC) \in (ABC)$$

がわかる. つまり,

$$D \times \mathrm{rad}(ABC) = ABC \times E$$

を満たす多項式 $E \in K[t]$ が存在する. 従って,

$$\deg(D) + \deg(\mathrm{rad}(ABC)) \geq \deg(ABC) \tag{5.2}$$

が成立する.

最後に, 式 (5.1) と式 (5.2) より

$$\max(\deg A, \deg B, \deg C) + \deg D < \deg D + \deg \mathrm{rad}(ABC)$$

が分かる. 整理すると

$$\max(\deg A, \deg B, \deg C) < \deg \mathrm{rad}(ABC)$$

となり, ABC 定理が証明された. □

5.2 ABC 定理の応用

定理 5.8. K は標数 0 の体とする. 正整数 p, q, r が $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$ を満たすとき,

$$X^p + Y^q = Z^r$$

を満たす多項式 $X, Y, Z \in K[t]$ で, 少なくとも一つは定数ではなく, どの二つも互いに素なものは存在しない.

証明. 仮定より, X, Y, Z はどれも 0 ではないことに注意する (よって $\deg X$, $\deg Y$, $\deg Z$ が定義できる).

背理法で示す. 定理にあるような X, Y, Z が存在すると仮定する.

$A = X^p, B = Y^q, C = Z^r$ として ABC 定理を適用すると,

$$\begin{aligned} \max(\deg(X^p), \deg(Y^q), \deg(Z^r)) &< \deg \mathrm{rad}(X^p Y^q Z^r) \\ &= \deg \mathrm{rad}(XYZ) \\ &\leq \deg(XYZ) \end{aligned}$$

を得る. すなわち,

$$p \deg(X) < \deg(XYZ)$$

$$q\deg(Y) < \deg(XYZ)$$

$$r\deg(Z) < \deg(XYZ)$$

の三式が成り立つ. それぞれを $\frac{1}{p}, \frac{1}{q}, \frac{1}{r}$ 倍して足し合わせると,

$$\deg(XYZ) = \deg(X) + \deg(Y) + \deg(Z) < (\frac{1}{p} + \frac{1}{q} + \frac{1}{r})\deg(XYZ)$$

となる. よって $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$ となり, 仮定に反する. □

定理 5.9. K は標数 0 の体とする. 整数 $m, n \geq 2$ に対し, $X^m - Y^n = 1$ を満たす定数でない多項式 $X, Y \in K[t]$ は存在しない.

証明. 背理法で示す. 定数でない多項式 X, Y で $X^m - Y^n = 1$ を満たすものがあると仮定する. このとき, $X^m, Y^n, 1$ はどの二つも互いに素である. $A = 1, B = Y^n, C = X^m$ として ABC 定理を適用すると,

$$\begin{aligned}\max(\deg(X^m), \deg(Y^n), 0) &< \deg \mathrm{rad}(X^m Y^n) \\ &= \deg \mathrm{rad}(XY) \\ &\leq \deg(XY)\end{aligned}$$

を得る. すなわち,

$$m\deg(X) < \deg(XY)$$

$$n\deg(Y) < \deg(XY)$$

の二式が成立する. それぞれを n, m 倍して足し合わせると,

$$mn(\deg(X) + \deg(Y)) < (m + n)\deg(XY)$$

となる. ここで, $\deg(X) > 0, \deg(Y) > 0$ より

$$\deg(X) + \deg(Y) = \deg(XY) > 0$$

がいえる. よって,

$$mn < m + n$$

であり, 整理すると

$$(m - 1)(n - 1) < 1$$

となる. これは $m, n \geq 2$ に矛盾する. □

この定理の整数における類似として, 次の定理が知られている.

定理 5.10. (カタラン (Catalan) 予想) 正整数 m, n, x, y で $x^m - y^n = 1$, $m, n \geq 2$ を満たすものは $(m, n, x, y) = (2, 3, 3, 2)$ だけである.

この定理はカタランにより 1844 年に予想され, 2002 年にミハイレスク (Mihăilescu) により証明された.

5.3 abc 予想

0 でない整数 a に対し, a の素因数すべての積を $\mathrm{rad}(a)$ と書く. すなわち,

$$\mathrm{rad}(a) = \prod_{p:a \text{ の素因数}} p$$

言い換えると, 相異なる素数 $p_1, \ldots, p_r$ と $e_1, \ldots, e_r \in \mathbb{Z}_{>0}$ について $a = \pm p_1^{e_1} \cdots p_r^{e_r}$ のとき, $\mathrm{rad}(a) = p_1 \cdots p_r$ である. ただし, $\mathrm{rad}(\pm 1) = 1$ と考える. 例えば

$$\mathrm{rad}(19800) = \mathrm{rad}(2^3 \times 3^2 \times 5^2 \times 11) = 2 \times 3 \times 5 \times 11 = 330$$

である. ABC 定理の整数における単純な類似は次のようになる.

0 でない整数 a, b, c がどの二つも互いに素で $a + b = c$ を満たすとき, 次の不等式は成り立つだろうか?

$$\max(|a|, |b|, |c|) < \mathrm{rad}(abc)$$

必要なら文字を入れ替えることで, a, b, c はすべて正としてよい. すると $a + b = c$ より $\max(|a|, |b|, |c|) = c$ となる. このとき,

$$\mathbf{abc} = \left\{ (a, b, c) \in \mathbb{Z}^3 \;\middle|\; \begin{array}{c} (a, b) = (b, c) = (c, a) = (1) \\ 0 < a < b < c,\ a + b = c \end{array} \right\}$$

とすると, 上記の問題は次のように言い換えられる.

任意の $(a, b, c) \in \mathbf{abc}$ に対し $c < \mathrm{rad}(abc)$ は成り立つだろうか? (abc-1)

しかし, (abc-1) には反例が存在する.

例 5.11. (i) $(a, b, c) = (1, 8, 9)$ のとき $9 > \mathrm{rad}(1 \times 8 \times 9) = 2 \times 3 = 6$ である.

(ii) $(a, b, c) = (5, 27, 32)$ のとき $32 > \mathrm{rad}(5 \times 27 \times 32) = 5 \times 3 \times 2 = 30$ である.

(iii) r を正整数として, $(a, b, c) = (1, 3^{2^r} - 1, 3^{2^r})$ とおく. このとき,

$$\begin{aligned} b = 3^{2^r} - 1 &= (3^{2^{r-1}})^2 - 1 = (3^{2^{r-1}} + 1)(3^{2^{r-1}} - 1) \\ &= \cdots = (3^{2^{r-1}} + 1)(3^{2^{r-2}} + 1) \cdots (3 + 1)(3 - 1) \end{aligned}$$

において, 最後の積の各因子はすべて偶数であり, $3+1=4$ なので, b は $2^r \times 4 = 2^{r+2}$ の倍数であることがわかる. したがって,

$$\mathrm{rad}(abc) = \mathrm{rad}((3^{2^r}-1)3^{2^r}) \leq \frac{3^{2^r}-1}{2^{r+1}} \times 3 < \frac{3}{2^{r+1}}c < c$$

となり, (abc-1) に反する.

ところが, (abc-1) を弱めた次の予想には反例が知られていない. しかし証明も知られていないので, すなわち未解決問題である.

予想 5.12. 次が成り立つような正整数 $N > 1$ が存在する.

$$\text{任意の } (a,b,c) \in \mathbf{abc} \text{ に対し } c < (\mathrm{rad}(abc))^N \text{が成り立つ} \qquad \text{(abc-N)}$$

注意 5.13. $N > 1$ を整数とする. このとき (abc-N) が成り立てば, $n \geq 3N$ に対するフェルマーの最終定理も成立する.

実際, n は $3N$ 以上の自然数とし, $x^n + y^n = z^n$, $x < y < z$ をみたし, どのふたつも互いに素な正整数 x, y, z が存在すると仮定する. $(a,b,c) = (x^n, y^n, z^n)$ として (abc-N) を用いると,

$$z^n < (\mathrm{rad}(x^n y^n z^n))^N = (\mathrm{rad}(xyz))^N \leq (xyz)^N < z^{3N}$$

となる. 従って, $n < 3N$ となり矛盾する.

次に予想 5.12 を詳しくみるため, 実数 $\kappa \geq 1$ に対し

$$\mathbf{abc}[\kappa] = \{(a,b,c) \in \mathbf{abc} \mid c \geq (\mathrm{rad}(abc))^\kappa\}$$

という集合を導入する. 定義より, $\kappa \leq \kappa'$ ならば $\mathbf{abc}[\kappa] \supset \mathbf{abc}[\kappa']$ が成り立つ. 何故ならば, $(a,b,c) \in \mathbf{abc}[\kappa']$ とすると, 定義より $c \geq (\mathrm{rad}(abc))^{\kappa'}$ となる. そして今, $\kappa \leq \kappa'$ より $c \geq (\mathrm{rad}(abc))^{\kappa'} \geq (\mathrm{rad}(abc))^\kappa$ がわかり, $(a,b,c) \in \mathbf{abc}[\kappa]$ がいえるからである.

例 5.11(iii) より, $\mathbf{abc}[1]$ は無限集合であることがわかる. 予想 5.12 は $\mathbf{abc}[N]$ が空集合となる $N > 1$ は存在するだろうかと問うている. つまり, $\mathbf{abc}[\kappa]$ は $\kappa = 1$ のとき無限集合であるが, κ が大きくなるごとに小さくなってゆき, いつかは空集合になると期待されているのである. 実際, $\kappa = 2$ の場合でも $\mathbf{abc}[2]$ に属する元は一つも知られていない. それより小さい $\kappa = 1.6$ については, $\mathbf{abc}[1.6]$ の元が 2018 年の時点で三つだけ発見されている.

$$(2, 3^{10} \times 109, 23^5) \qquad 1.62991\cdots,$$
$$(11^2, 3^2 \times 5^6 \times 7^3, 2^{21} \times 23) \qquad 1.62599\cdots,$$

$$(19 \times 1307, 7 \times 29^2 \times 31^8, 2^8 \times 3^{22} \times 5^4) \qquad 1.62349\cdots,$$

左側が **abc**[1.6] の元であり，一行目では $(a,b,c) = (2, 3^{10} \times 109, 23^5)$ のとき $c = \mathrm{rad}(abc)^{1.62991\cdots}$ になる，という意味である．**abc**[1.5] の元は 13 個だけ知られている．

予想 5.14. (**abc 予想**) 任意の実数 $\kappa > 1$ に対し **abc**[κ] は有限集合であろう．

この予想はエステルレ (Osterlé) とマッサー (Masser) により 1985 年に提出された．

定理 5.15. 予想 5.14. から予想 5.12 が従う．

証明． **abc**[2] が有限集合であると仮定する．

$$\mathbf{abc}[2] = \{(a,b,c) \in \mathbf{abc} \mid c \geq (\mathrm{rad}(abc))^2\} = \{(a_1,b_1,c_1), \cdots, (a_l,b_l,c_l)\}$$

とする．このとき，

$$d_i = \log_{\mathrm{rad}(a_i b_i c_i)} c_i$$

と定義する．変形すると，

$$c_i = (\mathrm{rad}(a_i b_i c_i))^{d_i}$$

となる．ここで，N は $N > \max\{d_1, \ldots, d_l, 2\}$ をみたす自然数とする．このとき，

$$\mathbf{abc}[N] \subset \mathbf{abc}[2]$$

である．ここで $(a_i, b_i, c_i) \in \mathbf{abc}[N]$ と仮定すると，

$$c_i \geq (\mathrm{rad}(a_i b_i c_i))^N$$

となる．しかし，先ほど定義した通り

$$c_i = (\mathrm{rad}(a_i b_i c_i))^{d_i}$$

であるので，$N \leq d_i$ となり，これは N のとり方に矛盾している．よって，

$$(a_i, b_i, c_i) \notin \mathbf{abc}[N]$$

がわかる．つまり，

$$\mathbf{abc}[N] = \phi$$

である．以上より，予想 5.12 が従う． □

予想 5.14 より精密に，例えば $\kappa = 1.6$ のときには **abc**[1.6] が上の三つの元だけからなると期待することもできる．今後新たな元が発見されるとしても有限個しかでてこない，

というのが abc 予想の述べていることだが, できれば「この三つしか例外はない」と言い切りたい. そこで「与えられた実数 $\kappa > 1$ に対し, $\mathbf{abc}[\kappa]$ の元は有限個で, しかもそのすべてをリストアップすることができる」という主張を**強い abc 予想**と呼ぶことにしよう.

予想 5.16. (**ビール (Beal) 予想**) p, q, r が 3 以上の整数ならば, どの二つも互いに素な正整数 x, y, z で $x^p + y^q = z^r$ を満たすものは存在しない.

定理 5.17. $\kappa = \frac{12}{11}$ に対する強い abc 予想を仮定すれば, ビール予想が解決, つまりビール予想が成立するか不成立かを確定することができる.

証明. $\kappa = \frac{12}{11}$ とおく. もし $\mathbf{abc}[\kappa]$ に 3 以上の整数 p, q, r に対して $(a, b, c) = (x^p, y^q, z^r)$ の形の元が入っていれば, ビール予想の反例となる. つまり, この場合ビール予想は不成立だとわかる.

以下このような元は存在しないと仮定する. このとき, ビール予想が正しいことを示そう. 背理法より, どの二つも互いに素な正整数 x, y, z と 3 以上の整数 p, q, r で $x^p + y^q = z^r$, $x^p < y^q < z^r$ を満たすものが存在したとする. $(a, b, c) = (x^p, y^q, z^r)$ は $\mathbf{abc}[\kappa]$ に属さない **abc** の元なので,

$$z^r < (\mathrm{rad}(x^p y^q z^r))^\kappa \leq (xyz)^\kappa$$

となる. よって,

$$x^p < y^q < z^r < (xyz)^\kappa$$

がわかる. つまり,

$$x < (xyz)^{\frac{\kappa}{p}}$$

$$y < (xyz)^{\frac{\kappa}{q}}$$

$$z < (xyz)^{\frac{\kappa}{r}}$$

の三式が得られる. これらをまとめると,

$$(xyz)^1 < (xyz)^{\frac{\kappa}{p}} (xyz)^{\frac{\kappa}{q}} (xyz)^{\frac{\kappa}{r}} = (xyz)^{\frac{\kappa}{p} + \frac{\kappa}{q} + \frac{\kappa}{r}}$$

となる. よって,

$$1 < \frac{\kappa}{p} + \frac{\kappa}{q} + \frac{\kappa}{r} = \frac{12}{11}\left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right) \tag{5.3}$$

が得られる. ここで $(p, q, r) = (3, 3, 3)$ のとき, フェルマーの最終定理より $x^3 + y^3 = z^3$ をみたす x, y, z は存在しない ($n = 3$ のときはオイラーによる初等的な証明がある). ま

た, $p,q,r \geq 3$ かつ $(p,q,r) \neq (3,3,3)$ なら $\frac{1}{p}+\frac{1}{q}+\frac{1}{r} \leq \frac{1}{3}+\frac{1}{3}+\frac{1}{4} = \frac{11}{12}$ が成り立つ. しかしこれは式 (5.3) に反し, このケースではビール予想は正しいとわかる.

以上より, ビール予想が解決されることがわかった. □

注意 5.18. abc 予想は次のように定式化されることが多い.

$$\begin{array}{l} \text{任意の } 1 < \kappa \in \mathbb{R} \text{ に対し, 実数 } M > 0 \text{ で, すべての} \\ (a,b,c) \in \mathbf{abc} \text{ に対し } c < M(\mathrm{rad}(abc))^{\kappa} \text{となるものが存在する.} \end{array} \tag{5.4}$$

これは予想 5.14 と同値である. 正確には,

命題 5.19. 任意の $1 < \kappa < \kappa'$ に対し次が成り立つ.

(i) κ に対する予想 5.14 から κ に対する (5.4) が従う.
(ii) κ に対する (5.4) から κ' に対する予想 5.14 が従う.

証明. まず (i) を示す. 予想 5.14 より, $\kappa \in \mathbb{R}_{>1}$ に対して $\mathbf{abc}[\kappa]$ は有限集合である. よって, $\mathbf{abc}[\kappa] = \{(a_1,b_1,c_1),\ldots,(a_n,b_n,c_n)\}$ と書ける. ここで,

$$M = \max\left\{ \frac{c_1}{(\mathrm{rad}(a_1b_1c_1))^{\kappa}}, \ldots, \frac{c_n}{(\mathrm{rad}(a_nb_nc_n))^{\kappa}} \right\} + 1$$

とおくと, すべての i に対して

$$\frac{c_i}{(\mathrm{rad}(a_ib_ic_i))^{\kappa}} < M$$

となる. 従って, (5.4) が従うとわかる.

次に (ii) を示す. ある $\kappa > 1$ に対して, (5.4) を仮定する. つまり, $M \in \mathbb{R}_{>0}$ ですべての $(a,b,c) \in \mathbf{abc}$ に対し $c < M(\mathrm{rad}(abc))^{\kappa}$ となるものが存在するとする. ここで, 予想 5.14 を示すため,

$$\kappa' > \kappa \text{ に対して } |\mathbf{abc}[\kappa']| < \infty$$

であることを示す.

$(a,b,c) \in \mathbf{abc}[\kappa']$ とすると, 定義より

$$c \geq (\mathrm{rad}(abc))^{\kappa'}$$

がわかる. ここで, $\kappa' > \kappa$ より $\mathbf{abc}[\kappa] \supset \mathbf{abc}[\kappa']$ である. よって, 仮定より

$$(\mathrm{rad}(abc))^{\kappa'} \leq c < M(\mathrm{rad}(abc))^{\kappa}$$

となる. よって, 一番左と一番右のみを考えて変形すると,

$$(\mathrm{rad}(abc))^{\kappa'-\kappa} < M$$

$$(\mathrm{rad}(abc))^{\kappa} < M^{\frac{\kappa}{\kappa'-\kappa}}$$

となる. 両辺に M をかけると,

$$c < M(\mathrm{rad}(abc))^{\kappa} < M^{\frac{\kappa}{\kappa'-\kappa}+1}$$

となり, 従って

$$c < M^{\frac{\kappa}{\kappa'-\kappa}+1}$$

が導き出される. このことから, $(a,b,c) \in \mathbf{abc}[\kappa']$ となる可能性がある c は有限個しかないことがわかる. すると, $0 < a < b < c$ より a, b も有限個だとわかるので, $\mathbf{abc}[\kappa']$ が有限集合であることが証明された. □

5.4 ロスの定理の強化版としての abc 予想

本節では, abc 予想がロスの定理の極めて自然な強力化であることを示していく.

ロスの定理は, $\rho > 2$ で, α が整数係数多項式の根ならば,

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^{\rho}}$$

を満たす既約分数 $\frac{p}{q}$ は有限個しかない, という主張であった. また, これを p 進絶対値に拡張したものも知られている. p を素数としたときに, p **進絶対値**とは,

$$\left|\pm p^k \times \frac{q}{r}\right|_p = p^{-k} \qquad (\text{ただし } (q,p) = (r,p) = 1)$$

と定義されたものであった (0 の p 進絶対値は 0 と定義する). p の高いべきで分子が割り切れるほど p 進絶対値は小さく, p の高いべきで分母が割り切れるほど p 進絶対値は大きい. また, 本節では便宜上通常の絶対値 $|x|$ を

$$|x|_{\infty}$$

とも書くことにし, $M = \{\text{ 素数 }\} \cup \{\infty\}$ という記号も用意する. このようにすることで, 通常の絶対値も p 進絶対値も統一的に

$$|x|_v \qquad (\text{ただし } v \in M)$$

と書けるようになる.

また, 既約分数 $\frac{q}{r}$ の**高さ** H は,

$$H\left(\frac{q}{r}\right) = \max(|q|, |r|)$$

であった. 実は, 1 未満となる絶対値の掛け算をすると, ちょうど x の高さの逆数になる. このことをまず次の命題で示そう.

命題 5.20. x を 0 ではない有理数とする. このとき,

$$\prod_{v \in M} \min(|x|_v, 1) = \frac{1}{H(x)} \tag{5.5}$$

証明. $x = \frac{q}{r}$ を既約分数表示とする.

$|q| \geq |r|$ のとき, $|\frac{q}{r}|_\infty \geq 1$ なので通常の絶対値は (5.5) 式の左辺に貢献しない. 1 より小さい絶対値を持つような p 進絶対値は分子 q を割り切る場合なので, q の素因数分解に p^k があるとき, $|x|_p = \frac{1}{p^k}$ となる. よって, このような素数を全て考えると, 1 より小さい部分の積は $\frac{1}{|q|}$ となる. 今の場合 $\max(|q|, |r|) = |q|$ だから, これは $\frac{1}{H(x)}$ に等しい.

逆に $|q| < |r|$ のとき, $|\frac{q}{r}|_\infty < 1$ である. p 進部分に関しては先ほどの場合と同様, 分子の素因数分解に p^k が登場するときに $\frac{1}{p^k}$ の絶対値を持つので, 全ての絶対値の情報を集めると

$$\frac{|q|}{|r|} \times \frac{1}{|q|} = \frac{1}{|r|}$$

となり, 今の場合 $\max(|q|, |r|) = |r|$ だから, これは $\frac{1}{H(x)}$ に等しい.

よって, 以上より題意は示された. □

次の命題は, 高さ関数の性質を表している.

$\mathbb{P}^1(\mathbb{Q})$ 上の点 $x = [x_0 : x_1]$ (ただし $x_0, x_1 \in \mathbb{Z}$, $\gcd(x_0, x_1) = 1$) に対して, $H(x) = \max\{|x_0|, |x_1|\}$ によって定義する.

命題 5.21. $a \in \mathbb{P}^1(\mathbb{Q})$ とする. このとき, a によって定まる定数 $C > 0$ が存在して, 任意の有理数 $x \neq a$ に対して,

$$H(x) \leq C \times H(x - a)$$

が成立する.

証明. $a = \infty = [1 : 0]$ のときは, $x = \frac{q}{r} = [\frac{q}{r} : 1]$ とすると,

$$H(x) = \max(|q|, |r|),$$

$$H(x-a) = H\left(\frac{1}{x}\right) = H\left(\frac{r}{q}\right) = \max(|r|,|q|)$$

なので, どの x に関しても $H(x) = H(x-a)$ となり, $C = 1$ ととればよい.

$a = \frac{\alpha}{\beta}$ とする. すると, $y = \frac{q}{r}$ が既約分数表示ならば,

$$H(y+a) = H\left(\frac{q}{r} + \frac{\alpha}{\beta}\right) = H\left(\frac{q\beta + \alpha r}{r\beta}\right)$$

となる. 分子は, 三角不等式より

$$|q\beta + \alpha r| \leq |q\beta| + |\alpha r| \leq (|\alpha| + |\beta|) \times \max(|q|,|r|)$$

となる. 一方分母は $|r\beta| \leq |\beta| \times \max(|q|,|r|)$ を満たす. よって $C = |\alpha| + |\beta|$ とおけば,

$$H(y+a) \leq C \times H(y)$$

がどの有理数 y でも満たされることがわかった. $\frac{q\beta+\alpha r}{r\beta}$ の分母と分子が約分されたとしても, さらに左辺が小さくなるので問題はない. 最後に $y = x - a$ を代入すれば,

$$H(x) \leq C \times H(x-a)$$

となるので, 証明できた. □

命題 5.21 は,「 a で動かしても高さはあまり変わらない」ということを言っている. C が x によらない定数であることがポイントである.

ロスの定理は, 次のように複数の絶対値に拡張できる. これは「リドゥーの定理」と呼ばれることもある. ロスの定理の主張から直接導くことは難しいものの, ロスの定理の証明方法をそのまま数の絶対値で行うことで得られる結果である.

定理 5.22. (ロスの定理の複数絶対値版 (リドゥーの定理)) S を M の有限部分集合とし, $a_1, \ldots, a_n \in \mathbb{P}^1(\mathbb{Q})$ とする. このとき $\rho > 2$ ならば,

$$\prod_{i=1}^{n}\left(\prod_{v\in S}\min(|x-a_i|_v, 1)\right) < \frac{1}{H(x)^\rho} \tag{5.6}$$

を満たすような有理数 x は有限個しかない (ただし, $x \neq a_1, \ldots, a_n$ として考える).

S の中に通常の絶対値が入っていてもいいし入っていなくてもよい. 「絶対値が小さい」ということは「x が a_i に近い」ということなので, S に含まれる絶対値で何らかの a_i に x が十分近いならば, そのような x の候補は有限個しかない, というのがこの定理の主張である. 一つの a_i に一つの絶対値でものすごく近いことによって (5.6) 式を満たすことも

可能だし, 複数の a_i や絶対値で「そこそこ」近いもの全部をまとめて (5.6) 式を満たすこともありうる. いずれにせよ x の候補は有限個となる, というのがこの定理の主張である.

さて, このリドゥーの定理を命題 5.20 や命題 5.21 を使って変形してみる. まず, 各 a_i ごとに命題 5.20 を $x - a_i$ に使うことで,

$$\prod_{v\in M} \min(|x-a_i|_v, 1) = \frac{1}{H(x-a_i)} \qquad (x \neq a_i)$$

がわかる. 次に, (5.6) 式の各 i ごとにこの式で割ると, リドゥーの定理を「式

$$\prod_{i=1}^{n} \left(\prod_{v\in M\setminus S} \min(|x-a_i|_v, 1)^{-1} \right) < \frac{1}{H(x)^\rho} \times \prod_{i=1}^{n} H(x-a_i) \tag{5.7}$$

を満たす有理数 x は有限個」という主張に変形できる. ここで, $K = \mathbb{P}^1(\mathbb{Q})\setminus\{a_1, \ldots, a_n\}$ として命題 5.21 を使うと, 各 a_i ごとにある $C_i > 0$ が存在して, $x \in K$ において

$$H(x) \leq C_i \times H(x-a_i)$$

が成り立つ. 変形すると,

$$\frac{1}{C_i} H(x) \leq H(x-a_i)$$

となる. よって,

$$\prod_{i=1}^{n} \left(\frac{1}{C_i} H(x) \right) \leq \prod_{i=1}^{n} H(x-a_i)$$

となるので, (5.7) 式型のリドゥーの定理から, 「式

$$\prod_{i=1}^{n} \left(\prod_{v\in M\setminus S} \min(|x-a_i|_v, 1)^{-1} \right) < \frac{1}{H(x)^\rho} \times \prod_{i=1}^{n} \left(\frac{1}{C_i} H(x) \right) = \frac{H(x)^{n-\rho}}{C_1 \cdots C_n}$$

を満たす有理数 x は有限個である」ことがわかる.

ここで, $a_1 = 0$, $a_2 = 1$. $a_3 = \infty$ の場合を考える. このときの $\frac{1}{C_1 C_2 C_3}$ を C と書くことにすると, 上の不等式は

$$\left(\prod_{v\in M\setminus S} \min(|x|_v, 1)^{-1} \right) \times \left(\prod_{v\in M\setminus S} \min(|x-1|_v, 1)^{-1} \right) \times \left(\prod_{v\in M\setminus S} \min(\left|\frac{1}{x}\right|_v, 1)^{-1} \right) < C \times H(x)^{3-\rho} \tag{5.8}$$

となる.

ここで, S に通常の絶対値を含めることにすると, $v \in M\backslash S$ はある素数 p に対する p 進絶対値となる. このとき, 有理数 α に対して

$$\min(|\alpha|_p, 1)^{-1} \tag{5.9}$$

の値を考えると, α の分母や分子に p のべきがないときは 1 , 分母に p のべきがあるときは $|\alpha|_p > 1$ より 1 , そして α の分子の素因数分解に p^k があるときは $\min(|\alpha|_p, 1) = \frac{1}{p^k}$ となるので, (5.9) 式は p^k となる. $\frac{1}{x}$ の分子は x の分母であることをふまえて (5.8) 式を書き直すと,

$$\left(\prod_{p\in M\backslash S}(|x| \text{ の分子の } p \text{ べき部分})\right) \times \left(\prod_{p\in M\backslash S}(|x-1| \text{ の分子の } p \text{ べき部分})\right) \times \left(\prod_{p\in M\backslash S}(|x| \text{ の分母の } p \text{ べき部分})\right) < C \times H(x)^{3-\rho} \tag{5.10}$$

となる.

リドゥーの定理から, (5.10) 式を満たすような有理数 $x \neq 0, 1$ は有限個しかない, ということがわかっている. 逆に言えば, 「式

$$\left(\prod_{p\in M\backslash S}(|x| \text{ の分子の } p \text{ べき部分})\right) \times \left(\prod_{p\in M\backslash S}(|x-1| \text{ の分子の } p \text{ べき部分})\right) \times \left(\prod_{p\in M\backslash S}(|x| \text{ の分母の } p \text{ べき部分})\right) \geq C \times H(x)^{3-\rho} \tag{5.11}$$

が有限個の例外を除いた有理数 x で必ず満たされる」ということである (例外に 0 や 1 も含める).

ここで, **根基** rad_p を, 0 でない整数 n に対して

$$\mathrm{rad}_p(n) = \begin{cases} p & (n \text{ が } p \text{ で割り切れるとき}) \\ 1 & (n \text{ が } p \text{ で割り切れないとき}) \end{cases}$$

と定義する. 予想 (5.11) よりも更に強い次のことが予想される.

$$\left(\prod_{p\in M\backslash S}\mathrm{rad}_p(|x| \text{ の分子})\right) \times \left(\prod_{p\in M\backslash S}\mathrm{rad}_p(|x-1| \text{ の分子})\right)$$

$$\times \left(\prod_{p \in M \setminus S} \mathrm{rad}_p(|x| \text{ の分母}) \right) \geq C \times H(x)^{3-\rho} \tag{5.12}$$

が有限個の例外を除いた有理数 x で必ず満たされる.

これが, abc 予想に関係した予想である. よく紹介される形に変形しよう. ρ はロス (リドゥー) の定理より 2 より大きい数だったので, ある正の数 ϵ を使って $\rho = 2 + \epsilon$ と記述できる. また, x を $\frac{a}{c}$ と既約分数表示して $b = c - a$ とおくと, a, b, c は共通の約数を持たない整数で, $a + b = c$ を満たす. また,

$$|x| \text{ の分子} = |a|, \quad |x-1| \text{ の分子} = \frac{|a-c|}{|c|} \text{の分子} = |b|, \quad |x| \text{ の分母} = |c|$$

である. また, $\gcd(a, b, c) = 1$ より

$$\mathrm{rad}_p(a) \times \mathrm{rad}_p(b) \times \mathrm{rad}_p(c) = \mathrm{rad}_p(abc)$$

も成り立つ. さらに, 三角不等式より $|b| \leq |a| + |c| \leq 2\max(|a|, |c|) = 2H(x)$ なので,

$$H(x) \leq \max(|a|, |b|, |c|) \leq 2H(x)$$

が成り立つ. 最後に, (5.11) 式を満たさないような有限個の x に対しては, この式の左辺と右辺の比をとることでどの定数 C' に変えたら成り立つのかを計算し, その中で一番小さいものを新しい C としてとってしまえばよい. $x \neq 0, 1$ である限り左辺は 0 にならず, 定義より $H(x)$ が ∞ になることはないので, C' は必ず 0 より大きくなり, 有限個の C' の最小値もやはり 0 より大きい. このように, C をより小さくすることで, 元々あった有限個の例外を (0 と 1 を除くと) なくすことができる. [19]

これらの観察を使って (5.11) 式を書き直したものが次の **abc 予想 2** である.

予想 5.23. (**abc 予想 2**) S を通常の絶対値を含むような M の有限部分集合とし, $\epsilon > 0$ とする. このとき, ある定数 $C > 0$ が存在して, 0 でない整数 a, b, c が $a + b = c$ かつ $\gcd(a, b, c) = 1$ を満たすならば,

$$\prod_{p \in M \setminus S} \mathrm{rad}_p(abc) \geq C \times \max(|a|, |b|, |c|)^{1-\epsilon}$$

が必ず成り立つ.

[19] $x = 0, 1$ のときは, それぞれ $a = 0$, $b = 0$ である.

つまり, 「$a+b=c$ という足し算の関係性を満たしている以上, 左辺が大きくなる」ということなので, abc を割り切るような十分大きい素数が存在することになる. 従って, 三つの数どれもが小さい素数だけからなるような素因数分解を持つことが不可能となる. 左辺が大きければよいので, 一つだけ大きい素数があってもいいし, そこそこの大きさの素数が十分な数あってもよい.

S を通常の絶対値のみとする場合,

$$\prod_{p\in M\setminus S}\mathrm{rad}_p(abc)=\prod_{p\text{ は素数}}\mathrm{rad}_p(abc)$$

となり, 右辺は $\mathrm{rad}(abc)$ と書かれ, abc を割り切る素数の積と等しくなる. 一般に, 定数 C は ϵ には依存し, ϵ を小さくすると C も小さくしないといけない. また, $C'=C^{\frac{-1}{1-\epsilon}}$, $1+\epsilon'=\frac{1}{1-\epsilon}$ とすることで,

$$C'\times\prod_{p\in M\setminus S}\mathrm{rad}_p(abc)^{1+\epsilon'}\geq\max(|a|,|b|,|c|)$$

の形となり (5.4) と同じ式になる.

5.5 abc 予想の応用

すでにいくつかの abc 予想の帰結を紹介したが, 本節ではディオファントス方程式への応用を紹介する. 元々フェルマーの最終定理への道具候補として考え出されたものだが, その他にも応用例はたくさん存在する. そのうちの代表的なものを紹介する.

abc 予想を仮定すると, ディオファントス方程式に関する重要な結果を直ちに得られてしまうことがよく分かるはずである. これは, これらのディオファントス方程式が簡単だからでなく, abc 予想が非常に強力だからである. 以下, その強力さを見ていきたいと思う.

n が十分大きいときのフェルマーの最終定理が abc 予想から導かれることは, 既に注意 5.13 で見た. ディオファントス方程式に関しても, 似たような議論で abc 予想から強い主張が得られる. まだ証明されていない結果で abc 予想の帰結となるものを紹介しようと思う.

予想 5.24. (フェルマー-カタラン予想) 自然数 x,y,z,k,m,n が

$$x^k+y^m=z^n,\quad \gcd(x,y,z)=1,\quad \frac{1}{k}+\frac{1}{m}+\frac{1}{n}<1 \tag{5.13}$$

を満たすような, 自然数の組 (x^k,y^m,z^n) は有限個しかない.

予想 5.16 (ビール予想) は, $k, l, m \geq 3$ のケースである.

この予想の名前は, フェルマーの最終定理 ($k = m = n \geq 4$ の場合) とカタラン予想のどちらも一般化していることに由来する. この予想はまだ未解決であるが, 今のところ知られている解は次のみである.

$$
\begin{aligned}
&1^l + 2^3 = 3^2 \quad (l \text{ は十分大きい自然数}), && 2^5 + 7^2 = 3^4, \\
&13^2 + 7^3 = 2^9, && 2^7 + 17^3 = 71^2, \\
&3^5 + 11^4 = 122^2, && 33^8 + 1549034^2 = 15613^3, \\
&1414^3 + 2213459^2 = 65^7, && 9262^3 + 15312283^2 = 113^7, \\
&17^7 + 76271^3 = 21063928^2, && 43^8 + 96222^3 = 30042907^2.
\end{aligned}
\tag{5.14}
$$

命題 5.25. abc 予想を仮定すると, フェルマー-カタラン予想を導くことができる. また, $\frac{1}{42}$ 未満のある一つの ϵ に対して abc 不等式が成り立つ定数 C を求められたら, (5.13) 式の解となりうる x^k, y^m, z^n の上界を求めることができる.

命題 5.25 の証明

以下, 自然数 x, y, z, k, m, n が (5.13) を満たすとする.

このとき, まず自然数 k, m, n が $\frac{1}{k} + \frac{1}{m} + \frac{1}{n} < 1$ であれば, $\frac{1}{k} + \frac{1}{m} + \frac{1}{n} \leq \frac{41}{42}$ を示す. 必要なら, k, m, n を入れかえることにより $k \leq m \leq n$ としてよい.

$k = 1$ としてみると,

$$\frac{1}{1} + \frac{1}{m} + \frac{1}{n} \geq 1$$

となってしまうので, $k = 1$ のものは存在しない.

$k = 2$, $m = 2$ としてみると,

$$\frac{1}{2} + \frac{1}{2} + \frac{1}{n} \geq 1$$

となってしまうので, このケースも存在しない.

$k = 2$, $m = 3$ のとき,

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{n} < 1$$

となる. これを変形すると $\frac{1}{n} < \frac{1}{6}$ となるので, $n > 6$ がわかる. 以上のことをふまえると,

$$\frac{1}{k} + \frac{1}{m} + \frac{1}{n} \leq \frac{1}{2} + \frac{1}{3} + \frac{1}{7} = \frac{41}{42}$$

が得られる.

次に, $k=2$, $m \geq 4$ のケースを考える. このとき,

$$\frac{1}{2}+\frac{1}{m}+\frac{1}{n} \leq \frac{1}{2}+\frac{1}{4}+\frac{1}{n}=\frac{3}{4}+\frac{1}{n}$$

となる. よって, $\frac{1}{k}+\frac{1}{m}+\frac{1}{n}<1$ より

$$\frac{3}{4}+\frac{1}{n}<1$$

となり, $\frac{1}{n}<\frac{1}{4}$ がわかる. よって, $n>4$ となる. 以上のことをふまえると,

$$\frac{1}{k}+\frac{1}{m}+\frac{1}{n} \leq \frac{1}{2}+\frac{1}{4}+\frac{1}{5}=\frac{19}{20}<\frac{41}{42}$$

が得られる.

次に, $k=3$, $m=3$ のケースを考える.

$$\frac{1}{3}+\frac{1}{3}+\frac{1}{n}<1$$

より $\frac{1}{n}<\frac{1}{3}$ となるので, $n>3$ となる. 以上のことをふまえると,

$$\frac{1}{3}+\frac{1}{3}+\frac{1}{4} \leq \frac{11}{12}<\frac{41}{42}$$

が得られる.

次に, $k=3$, $m \geq 4$ のケースを考える.

$$\frac{1}{3}+\frac{1}{m}+\frac{1}{n} \leq \frac{1}{3}+\frac{1}{4}+\frac{1}{n}=\frac{7}{12}+\frac{1}{n}$$

となる. よって, $\frac{1}{k}+\frac{1}{m}+\frac{1}{n}<1$ より

$$\frac{7}{12}+\frac{1}{n}<1$$

となり, $\frac{1}{n}<\frac{5}{12}$ がわかる. よって, $n \geq m$ と合わせて $n \geq 4$ となる. 以上のことをふまえると,

$$\frac{1}{k}+\frac{1}{m}+\frac{1}{n} \leq \frac{1}{3}+\frac{1}{4}+\frac{1}{4}=\frac{5}{6}<\frac{41}{42}$$

が得られる.

最後に, $k \geq 4$ のケースを考える. このとき, $k \leq m \leq n$ より, $m \geq 4$, $n \geq 4$ である. よって,

$$\frac{1}{k}+\frac{1}{m}+\frac{1}{n} \leq \frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}<\frac{41}{42}$$

が得られる.

以上より, $\frac{1}{k}+\frac{1}{m}+\frac{1}{n}<\frac{41}{42}$ が示された.

$\gcd(x,y,z)=1$ なので $x^k=a$, $y^m=b$, $z^n=c$ とおいて abc 予想を適用する. すると,

$$C\max\{a,b,c\}^{1-\epsilon}<\mathrm{rad}(x^ky^mz^n)=\mathrm{rad}(xyz)\leq xyz$$

を満たす $0<\epsilon<1$ と $C>0$ をとれる. すると,

$$\begin{aligned}\left(\frac{xyz}{C}\right)^{\frac{1}{k}}&\geq x^{1-\epsilon}\\ \left(\frac{xyz}{C}\right)^{\frac{1}{m}}&\geq y^{1-\epsilon}\\ \left(\frac{xyz}{C}\right)^{\frac{1}{n}}&\geq z^{1-\epsilon}\end{aligned}\tag{5.15}$$

が得られる. (5.15) 式の矢印の右側を掛け合わせると,

$$\left(\frac{1}{C}\right)^{\frac{1}{k}+\frac{1}{m}+\frac{1}{n}}\times(xyz)^{\frac{1}{k}+\frac{1}{m}+\frac{1}{n}}>(xyz)^{1-\epsilon}$$

となる. ここで, $\frac{1}{k}+\frac{1}{m}+\frac{1}{n}\leq\frac{41}{42}$ を使うと, C は十分小さい正の実数なので,

$$\left(\frac{1}{C}\right)^{\frac{41}{42}}\times(xyz)^{\frac{1}{k}+\frac{1}{m}+\frac{1}{n}}>(xyz)^{1-\epsilon}$$

を得る. $\left(\frac{1}{C}\right)^{\frac{41}{42}}=C'$ とおく. このとき, $\epsilon<\frac{1}{42}$ ならば $\frac{1}{k}+\frac{1}{m}+\frac{1}{n}\leq\frac{41}{42}<1-\epsilon$ である. よって,

$$C'>(xyz)^{1-\epsilon-\left(\frac{1}{k}+\frac{1}{m}+\frac{1}{n}\right)}\geq(xyz)^{1-\epsilon-\frac{41}{42}}=(xyz)^{\frac{1}{42}-\epsilon}$$

となり, $(C')^{\frac{1}{\frac{41}{42}-\epsilon}}>xyz$ となる. もう一度 (5.15) に戻ると,

$$\begin{aligned}xyz&\geq C\times(x^k)^{1-\epsilon}\\ xyz&\geq C\times(y^m)^{1-\epsilon}\\ xyz&\geq C\times(z^n)^{1-\epsilon}\end{aligned}$$

となるので, x^k, y^m, z^n を探す範囲が定まる. 具体的には,

$$\left(\frac{1}{C}\times(C')^{\frac{1}{\frac{1}{42}-\epsilon}}\right)^{\frac{1}{1-\epsilon}}$$

以下を探せば良いとわかる. □

次に紹介するのは, ピライが 1931 年に立てた予想である.

予想 5.26. (ピライ予想) p, q, r を自然数とする. このとき,

$$px^m - qy^n = r, \quad m \geq 2, \quad n \geq 2, \quad (m, n) \neq (2, 2)$$

を満たす自然数の組 (x, y, m, n) は有限個である.

$m = n = 2$ の場合は, 例えば $p = 1$, $q = 2$, $r = 1$ とおくとペル方程式となる. 定理 3.1 で見たように, ペル方程式は無限個の解を持つ.

命題 5.27. abc 予想を仮定すると, ピライ予想を示すことができる.

証明. (x, y, m, n) は, 与えられた条件を満たす自然数の組とする. $\gcd(px^m, qy^n) = d$ とする. このとき, d は r の約数なので $d \leq r$ に注意する.

$$\mathrm{rad}(\frac{px^m}{d} \times \frac{qy^n}{d} \times \frac{r}{d}) \leq \mathrm{rad}(px^m \times qy^n \times r) \leq pqrxy$$

を用いると, abc 予想より

$$\begin{aligned}
pqrxy > C \times (\frac{px^m}{d})^{1-\epsilon} \qquad &\text{から} \qquad (\frac{pqrd^{1-\epsilon}xy}{Cp^{1-\epsilon}})^{\frac{1}{m}} \geq x^{1-\epsilon}, \\
pqrxy > C \times (\frac{qy^n}{d})^{1-\epsilon} \qquad &\text{から} \qquad (\frac{pqrd^{1-\epsilon}xy}{Cq^{1-\epsilon}})^{\frac{1}{n}} \geq y^{1-\epsilon} \qquad (5.16) \\
\left(\frac{pqrd^{1-\epsilon}}{Cp^{1-\epsilon}}\right)^{\frac{1}{m}} \geq x^{1-\epsilon-\frac{1}{m}} y^{-\frac{1}{m}}, \qquad &\left(\frac{pqrd^{1-\epsilon}}{Cq^{1-\epsilon}}\right)^{\frac{1}{n}} \geq x^{-\frac{1}{n}} y^{1-\epsilon-\frac{1}{n}}
\end{aligned}$$

がいえる. 条件より $\frac{1}{m} + \frac{1}{n} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$ なので,

$$\begin{aligned}
\max(\frac{pqrd^{1-\epsilon}}{Cp^{1-\epsilon}}, \frac{pqrd^{1-\epsilon}}{Cq^{1-\epsilon}})^{\frac{5}{6}} &\geq (\frac{pqrd^{1-\epsilon}}{Cp^{1-\epsilon}})^{\frac{1}{m}} (\frac{pqrd^{1-\epsilon}}{Cq^{1-\epsilon}})^{\frac{1}{n}} \\
&\geq (xy)^{1-\epsilon-\frac{1}{m}-\frac{1}{n}} \\
&\geq (xy)^{1-\epsilon-\frac{5}{6}}
\end{aligned}$$

がわかる. $d \leq r$ より, 上の不等式から xy の上界が求まる. そこで, (5.16) に戻ると x^m や y^n の上界も求まるので, x, y, m, n は有限個であるとわかる. □

ピライ予想は, 「べき数の差が, ある固定された数になることはあまりないだろう」という予想である. 言い換えると, これは「べき数の差は結構大きくならなければならない」ということになる. この形で書かれたものが次のホール-ラング-ヴァイルシュミット-スピロ予想で, これも abc 予想からすぐに導ける.

予想 5.28. (**ホール-ラング-ヴァルトシュミット-スピロ予想**) m, n を 2 以上の自然数とし, $\epsilon > 0$ とする. このとき, ある定数 $C' > 0$ が存在して, x, y, z が自然数で $x^m - y^n = z \neq 0$ かつ $\gcd(x, y) = 1$ を満たすならば,

$$x^{mn-m-n} < C' \times \mathrm{rad}(z)^{n+\epsilon}$$
$$y^{mn-m-n} < C' \times \mathrm{rad}(z)^{m+\epsilon}$$

が成り立つ.

$\mathrm{rad}(z) \leq z$ なので, 特に, べき数の差は大きい, と主張している. 右辺の $\mathrm{rad}(z)$ を z で置き換えて主張を弱くしたもののことを, **ホール-ラング-ヴァルトシュミット予想**と呼ぶこともある. 特に重要なのが, $m = 3$, $n = 2$ の場合で, この場合のホール-ラング-ヴァルトシュミット予想

$$x < C' z^{2+\epsilon}, \quad y < C' z^{3+\epsilon}$$

は**ホール予想**, この場合のホール-ラング-ヴァルトシュミット-スピロ予想

$$x < C' \mathrm{rad}(z)^{2+\epsilon}, \quad y < C' \mathrm{rad}(z)^{3+\epsilon}$$

(つまり, $\max(x^3, y^2) < C'' \times \mathrm{rad}(z)^{6+\epsilon}$) は**強いホール予想**と呼ばれる.

命題 5.29. abc 予想を仮定すると, ホール-ラング-ヴァルトシュミット-スピロ予想を導ける.

証明. $\epsilon > 0$ が与えられたとする. m と n は固定されているので,

$$\min\left(\frac{n+\epsilon}{n}, \frac{m+\epsilon}{m}\right) > \frac{mn-m-n}{mn-m-n-\epsilon' mn} \tag{5.17}$$

を満たすように正の ϵ' を取ることができる. ここで, $\mathrm{rad}(x^m \times y^n \times z) \leq xy \times \mathrm{rad}(z)$ であるので, この ϵ' の場合の abc 予想を使うと,

$$\mathrm{rad}(z) \times xy \geq C \max(x^m, y^n)^{1-\epsilon'}$$

がわかる. また, $x \leq \max(x^m, y^n)^{\frac{1}{m}}$, $y \leq \max(x^m, y^n)^{\frac{1}{n}}$ を使うと,

$$\mathrm{rad}(z) \geq C \times \frac{\max(x^m, y^n)^{1-\epsilon'}}{xy} \geq C \times \max(x^m, y^n)^{1-\frac{1}{m}-\frac{1}{n}-\epsilon'}$$

となる ($C > 0$). よって,

$$\mathrm{rad}(z)^n \geq C^n (x^{mn})^{1-\frac{1}{m}-\frac{1}{n}-\epsilon'} = C^n x^{mn-m-n-\epsilon' mn}$$

$$\mathrm{rad}(z)^m \geq C^m (y^{mn})^{1-\frac{1}{m}-\frac{1}{n}-\epsilon'} = C^m y^{mn-m-n-\epsilon' mn}$$

がわかる. 上の式の左辺を (5.17) 式の左辺でべき乗, 上の式の右辺を (5.17) 式の右辺でべき乗すると,

$$\mathrm{rad}(z)^{n+\epsilon} > C^{\frac{mn^2-mn-n^2}{mn-m-n-\epsilon' mn}} x^{mn-m-n} \tag{5.18}$$

$$\mathrm{rad}(z)^{m+\epsilon} > C^{\frac{m^2n-mn-m^2}{mn-m-n-\epsilon' mn}} y^{mn-m-n} \tag{5.19}$$

となる. 従って,

$$C' = \min\left(C^{\frac{mn^2-mn-n^2}{mn-m-n-\epsilon' mn}}, C^{\frac{m^2n-mn-m^2}{mn-m-n-\epsilon' mn}} \right)$$

とおけば, 題意が示される. □

参考文献

[1] 安福 悠発見・予想を積み重ねる —それが整数論, オーム社, 2016.

[2] 山崎隆雄初等整数論 —数論幾何への誘い—共立講座 数学探検 6, 2015.