

フェルマー予想と ABC 予想

山崎隆雄 (東北大学)

整数と多項式には多くの共通する性質がある。和・差・積が定義される (しかし商は必ずしも定義されない) ということを出発点として、約数・倍数・素数・素因数分解などの基本概念が平行した方法で扱えることが顕著である。そこで、整数論の有名問題、特にフェルマー予想を取り上げて、その多項式に対する類似を考える。講義では、この問題に対して「ABC 定理」を経由した証明を解説する。この ABC 定理は多項式に対する定理であるが、その整数における類似を考えると、これが abc 予想という未解決問題にたどり着く。その周辺の話題を紹介する。

この原稿は、以下で行った講義が元になっている：

- 現代数学講演会 (2007年12月18日、於仙台第一高等学校)
- JMO 夏季セミナー (2008年8月26日、於山梨県清里高原「ヴィラ千ヶ滝」)
- 数学概説 B (2009・2010年、於東北大学)
- 科学者の卵養成講座 (2010年6月12日、於東北大学)

1. フェルマー予想

定理 1.1. n が 3 以上の整数のとき、 $x^n + y^n = z^n$ は「自明でない」整数の解を持たない。

注意 1.2. • 「自明な解」とは、 x, y, z のいずれかが 0 の解。例： $(x, y, z) = (2, 0, 2)$ 。

- 予想は 1630 年ごろフェルマーが述べた。1994 年にワイルズが証明した [14]。
- $n = 2$ のときは無数に解がある。例： $3^2 + 4^2 = 5^2, 15^2 + 8^2 = 17^2$ 。

この講義の一つの目標は次の定理の証明である：

定理 1.3. n が 3 以上の整数のとき、 $X(t)^n + Y(t)^n = Z(t)^n$ を満たす多項式 $(X(t), Y(t), Z(t))$ は「自明なもの」しかない。

注意 1.4. • 「自明な解」とは、 $a^n + b^n = c^n$ を満たす定数 a, b, c と、ある多項式 $W(t)$ によって $X(t) = aW(t), Y(t) = bW(t), Z(t) = cW(t)$ と表される解。例： $(a, b, c) = (1, 1, \sqrt[n]{2})$ 。

- はじめに証明したのはリュール (1851 年) より前。
- $n = 2$ のときは無数に解がある。例： $(t^2 - 1)^2 + (2t)^2 = (t^2 + 1)^2$ 。この例で $t = 2, 4$ を代入したのが、フェルマー予想の $n = 2$ で挙げた例。
- 「定数」「多項式」などの語の意味は、次の節でもう少し精密に述べる。

この問題が面白いのは、整数と多項式の高度な類似が成り立つことにある。その様子を次の節で述べる。次に「ABC 定理」を紹介し、定理 1.3 (および類似の定理) を証明する。その後に「ABC 定理」を証明する。「ABC 定理」の整数における類似は「abc 予想」という未解決問題である。最後に、この予想が解ければ (多項式のときと同じようにして) 定理 1.1 の (別) 証明が与えられることなどを解説する。

定理 1.3 の証明に関係するのは 2, 5, 6 章だけである。これらだけを読むこともできる。

2. 素因数分解

2.1. 整数. 整数全体の集合を $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ と書く。

- $a, b \in \mathbb{Z}$ ならば $a \pm b, ab \in \mathbb{Z}$ である。(しかし $b \neq 0$ であっても $a/b \in \mathbb{Z}$ とは限らない。)
[もちろん結合法則などの諸性質を満たす [整域である] が、ここでは復習しない。]
- $a, b \in \mathbb{Z}, b \neq 0$ ならば $a = bq + r, 0 \leq r < |b|$ を満たす $q, r \in \mathbb{Z}$ が (唯一) 存在する。
- 上で $r = 0$ のとき $b|a$ と書き、 b は a の約数という。
- 1 の約数は ± 1 のみである。これらを単数という。
- $p \in \mathbb{Z} \setminus \{\pm 1\}$ が $\pm 1, \pm p$ しか約数を持たないとき素元という。さらに $p > 0$ なら素数という。

定理 2.1. a を 0 でも単数でもない整数とする。このとき、素元 p_1, \dots, p_r で

$$a = p_1 p_2 \cdots p_r$$

を満たすものが存在する。さらに、この表示は次の意味で一意的である：もしも

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad (p_1, \dots, p_r, q_1, \dots, q_s : \text{素元})$$

ならば、 $r = s$ であり、 q_1, \dots, q_r の番号づけと符号をうまく選べば $p_1 = \pm q_1, \dots, p_r = \pm q_r$ となる。

いろいろなところで符号が出てきて邪魔であったが、これがちょうど「単数倍」であることに注意。

2.2. 多項式. 多項式全体の集合を $\mathbb{R}[t] = \{\sum_{n=0}^r a_n t^n \mid a_n \in \mathbb{R}\}$ と書く。(\mathbb{R} は実数全体の集合。)

- $A(t), B(t) \in \mathbb{R}[t]$ ならば $A(t) \pm B(t), A(t)B(t) \in \mathbb{R}[t]$ である。
- $A, B \in \mathbb{R}[t], B \neq 0$ ならば、 $A = BQ + R$ かつ「 $R = 0$ または $\deg R < \deg B$ 」を満たす $Q, R \in \mathbb{R}[t]$ が存在する。ただし、ゼロでない多項式 $C(t) = \sum_{n=0}^r c_n t^n$ ($c_r \neq 0$) に対して $\deg C(t) = r$ は $C(t)$ の次数である。
- 上で $R = 0$ のとき $B|A$ と書き、 B は A の約数という。
- 1 の約数となる多項式は 0 以外の定数のみである。これらを単数という。
- 定数でない多項式 $P \in \mathbb{R}[t]$ で、定数と P の定数倍以外の約数を持たないものを素元と呼ぶ。
- 二つの素元 P, Q に対し $P = uQ$ となる単数 u が存在するとき P と Q は同伴と呼ぶ。

定理 2.2. $A(t)$ を 0 でも単数でもない多項式とする。このとき、素元 P_1, \dots, P_r で

$$A = P_1 P_2 \cdots P_r$$

を満たすものが存在する。さらに、この表示は次の意味で一意的である：もしも

$$A = P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s \quad (P_1, \dots, P_r, Q_1, \dots, Q_s : \text{素元})$$

ならば、 $r = s$ であり、 Q_1, \dots, Q_r の番号づけをうまく選べば P_i と Q_i は同伴 ($i = 1, \dots, r$) となる。

注意 2.3. • 整数の絶対値 $|a|$ の役割は多項式では次数 $\deg A$ が担っている。

- 「定数」は実数 \mathbb{R} でなく、複素数 \mathbb{C} や有理数 \mathbb{Q} [より一般に体] としても構わない。
- ただし、 \mathbb{R} を \mathbb{Z} に置き換えた「整数係数の多項式 $\mathbb{Z}[t]$ 」や、 \mathbb{R} を $\mathbb{R}[s]$ に置き換えた「二変数の多項式 $\mathbb{R}[s, t]$ 」を考えると大きく事情が変わる。(\mathbb{Z} や $\mathbb{R}[s]$ は除法が自由にできないから。)
- $\mathbb{R}[t]$ の素元は分類できる： $t + a$ と $t^2 + bt + c$ ($a, b, c \in \mathbb{R}, b^2 - 4c < 0$) の単数倍。
- $\mathbb{C}[t]$ の素元も分類できる： $t + a$ ($a \in \mathbb{C}$) の単数倍。(定理 9.1 で再び取り上げる。)
- $\mathbb{Q}[t]$ の素元は非常に複雑。

2.3. ガウス整数. $i = \sqrt{-1}$ を虚数単位として $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ と書く. これは \mathbb{C} の部分集合.

- $\alpha, \beta \in \mathbb{Z}[i]$ ならば $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[i]$ である. (しかし $\beta \neq 0$ でも $\alpha/\beta \in \mathbb{Z}[i]$ とは限らない.)
- $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$ ならば $\alpha = \beta\kappa + \rho, 0 \leq \|\rho\| < \|\beta\|$ を満たす $\kappa, \rho \in \mathbb{Z}[i]$ が存在する. ここで $a, b \in \mathbb{R}$ に対し $\|a + bi\| = a^2 + b^2$ と書いた. (例題 2.4 を参照.)
- 上で $\rho = 0$ のとき $\beta|\alpha$ と書き, β は α の約数という.
- 1 の約数は $\pm 1, \pm i$ の四つある. これらを単数という.
- 単数でない $\pi \in \mathbb{Z}[i]$ で, 約数が $\epsilon, \pi\epsilon$ (ϵ : 単数) しかないものを素元と呼ぶ.
- 二つの素元 π, π' に対し $\pi' = \epsilon\pi$ となる単数 ϵ が存在するとき π と π' は同伴と呼ぶ.

例題 2.4. (1) 任意の $\xi \in \mathbb{C}$ に対し $\|\xi - \kappa\| \leq 1/2 (< 1)$ を満たす $\kappa \in \mathbb{Z}[i]$ が存在することを示せ.
 (2) $\xi = \alpha/\beta$ に対して (1) を適用することで「割り算」の存在を示せ.

定理 2.5. $\alpha \in \mathbb{Z}[i]$ を 0 でも単数でもない元とする. このとき, 素元 π_1, \dots, π_r で

$$\alpha = \pi_1\pi_2 \cdots \pi_r$$

を満たすものが存在する. さらに, この表示は次の意味で一意的である: もしも

$$\alpha = \pi_1 \cdots \pi_r = \pi'_1 \cdots \pi'_s \quad (\pi_1, \dots, \pi_r, \pi'_1, \dots, \pi'_s : \text{素元})$$

ならば, $r = s$ であり, π'_1, \dots, π'_r の番号づけうまく選べば π_i と π'_i は同伴 ($i = 1, \dots, r$) となる.

注意 2.6. • 普通の (\mathbb{Z} の) 素数 p は $\mathbb{Z}[i]$ の元と思うときに素元となることもならないこともある. 例えば $5 = (1 + 2i)(1 - 2i)$ なので 5 は $\mathbb{Z}[i]$ の素元ではない. ($1 \pm 2i$ は素元となる.)
 $13 = (3 + 2i)(3 - 2i)$ も同様. $3, 7, 11$ は $\mathbb{Z}[i]$ においても素元となることが証明できる.
 • そのため, 「素因数分解」も \mathbb{Z} におけるものと $\mathbb{Z}[i]$ におけるものは様子が異なる. 例:

$$6 = (1 + i)(1 - i)3, \quad -1 + 8i = (1 + 2i)(3 + 2i)$$

例題 2.7. (1) 60 と 260 を \mathbb{Z} および $\mathbb{Z}[i]$ で素因数分解せよ.
 (2) $t^4 - 1$ と $t^4 + 1$ を $\mathbb{R}[t]$ および $\mathbb{C}[t]$ で素因数分解せよ.

2.4. その他の例と反例.

- $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ において, 単数が ± 1 の二つだけとなることを除けばまったく同じことが成り立つ. (例題 2.4 (1) において $\mathbb{Z}[i]$ を $\mathbb{Z}[\sqrt{-2}]$ に置き換えれば「割り算」の存在も同様に示すことができる.)
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ では「割り算」が存在せず (例題 2.4 (1) において $\mathbb{Z}[i]$ を $\mathbb{Z}[\sqrt{-5}]$ に置き換えると成り立たなくなる), 「素因数分解の一意性」も成り立たない. 例えば

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

となるが $2, 3, 1 \pm \sqrt{-5}$ は単数を除くとそれ以上分解できないという意味で「素元」となる. (既約元という方が正確.)

- 一般に, $d \in \mathbb{Z}$ とするとき $\mathbb{Z}[\sqrt{d}]$ において「素因数分解の一意性」が成り立つかどうかは非常に微妙な問題である.
- $\mathbb{C}[t, \sqrt{1-t^2}] = \{A(t) + B(t)\sqrt{1-t^2} \mid A, B \in \mathbb{C}[t]\}$ では「素因数分解の一意性」が成り立つ.
 $\mathbb{C}[t, \sqrt{1-t^3}] = \{A(t) + B(t)\sqrt{1-t^3} \mid A, B \in \mathbb{C}[t]\}$ では成り立たない. 命題 10.9 を参照.

2.5. 証明. 上に述べた定理はどれもまったく同じように証明ができる。(証明で用いる重要な性質は割り算の原理。)ここでは多項式に限定して証明を与える。

証明に入る前に、多項式の次数について簡単な注意。 A, B がゼロでない多項式のとき

- $\deg(AB) = \deg A + \deg B$ が成り立つ。[$\mathbb{Z}, \mathbb{Z}[i]$ の場合、 $|ab| = |a| \cdot |b|$ または $\|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$.]
- $\deg A = 0 \Leftrightarrow A$ は単数。[$\mathbb{Z}, \mathbb{Z}[i]$ の場合、 $|a| = 1$ または $\|\alpha\| = 1 \Leftrightarrow$ 単数。]

ゼロでも単数でもない元 $A(t) \in \mathbb{R}[t]$ を取る。上の注意より $\deg A > 0$ である。以下、 $\deg A$ に関する帰納法で証明する。

(分解の存在) A が素元ならば $r = 1, P_1 = A$ が定理にいう分解を与える。 A が素元でなければ、素元の定義から定数でない多項式 B, C により $A = BC$ と分解される。この式より $\deg B, \deg C < \deg A$ 。帰納法の仮定により B, C は素元の積に分解される。従って $A = BC$ も分解される。

(分解の一意性) 素元 $P_1, \dots, P_r, Q_1, \dots, Q_s$ について

$$(!) \quad A = P_1 \cdots P_r = Q_1 \cdots Q_s$$

が成り立つと仮定する。まず、ある組 (i, j) について P_i と Q_j が同伴である、すなわち $P_i = uQ_j$ となる単数 u があるときを考える。 $i = j = 1$ としてよい。すると $A/P_1 = A/uQ_1 = P_2 \cdots P_r = u^{-1}Q_2 \cdots Q_s$ に対して帰納法の仮定を適用すれば定理の後半の主張(分解の一意性)を得る。次に

$$(*) \quad \text{すべての組 } (i, j) \text{ に対して } P_i \neq Q_j$$

の場合を考える。さらに(必要なら P と Q の名前を付け替えて) $\deg P_1 \leq \deg Q_1$ を仮定する。ここで「割り算」を実行すると、多項式 S, T で

$$(**) \quad Q_1 = SP_1 + T \text{ かつ } T = 0 \text{ または } 0 \leq \deg T < \deg P_1 (\leq \deg Q_1)$$

を満たすものが存在する。 $T = 0$ ならば $Q_1 = SP_1$ となり、(P_1, Q_1 は素元だから) S は単数、 P_1 と Q_1 が同伴となり $(*)$ に反する。 $T \neq 0$ のときは、 $(!)$ によって $P_1 \cdots P_r = (SP_1 + T)Q_2 \cdots Q_s$ 、すなわち

$$P_1(P_2 \cdots P_r - SQ_2 \cdots Q_s) = TQ_2 \cdots Q_s$$

を得る。 $(**)$ より右辺は次数が $< \deg A$ なので帰納法の仮定より分解の一意性が成立する。左辺が P_1 で割れることから右辺もそうなる。しかし、 $P_1|T$ は次数の条件 $(**)$ に反し、 $P_1|Q_j$ ($j = 2, \dots, s$) は $(*)$ に反する。□

例題 2.8. 定理 2.1, 2.5 を証明せよ。また、文献をあたって別の証明を調べよ。(上で述べた証明は標準的ではない。)

いったん「素因数分解の一意性」を確立してしまえば、整数の場合と同じようにして(最小)公倍数・(最大)公約数・互いに素.....など概念が定義できる。以下、自由にその種の用語を用いることにする。

3. PYTHAGORAS の発見と MERSENNE/FERMAT 数

この章はとばしても構わない。素因数分解の簡単な応用をいくつか紹介する。

定理 3.1 (Pythagoras?). $x^2 = 2y^2$ を満たす $x, y \in \mathbb{Z} \setminus \{0\}$ は存在しない。つまり、 $\sqrt{2}$ は無理数。

証明. 両辺の素因数分解において 2 の指数を比較する。 □

次の定理はこの一般化となっている：

定理 3.2. $x, y \in \mathbb{Z} \setminus \{0\}$ が互いに素で $x^n + a_{n-1}x^{n-1}y + a_{n-2}x^{n-2}y^2 + \cdots + a_0y^n = 0$ を満たす $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$ が存在するなら $y = \pm 1$ である。

証明. $y \neq \pm 1$ ならば $p|y$ なる素数 p が存在する。仮定の式から $p|x^n$ を、従って $p|x$ を得るが、これは「互いに素」の仮定に反する。 □

$z = x/y$ とおけば、「有理数 z が $z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0$ を満たすなら z は整数」ということである。代数学の言葉では、この事実を「 \mathbb{Z} は整閉である」と表現する。

命題 3.3. $n, a > 1$ とする。 $a^n - 1$ が素数なら $a = 2$ で n も素数。

証明. $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ が素数なので $a = 2$ 。また、 $n = kl$ なら $2^{kl} - 1 = (2^k)^l - 1 = (2^k - 1)((2^k)^{l-1} + \cdots + 1)$ 。 □

定義 3.4. p を素数とすると $M_p = 2^p - 1$ を Mersenne 数という。

$M_2 = 3, M_3 = 7, M_5 = 31, M_7, M_{13}, M_{17}, \dots, M_{43112609}$ は素数。 $M_{11} = 2047 = 23 \cdot 89$ は素数でない。 M_p が素数となる p が有限個かどうかは未解決。2009年7月までに47個だけ素数となるものが見つかっている。(上に挙げた最後のものはそのうち最大。) M_p が素数なら $M_p(M_p + 1)/2$ は偶数の完全数で、偶数の完全数はこれらに限る。奇数の完全数が存在するかどうかは知られていない。

命題 3.5. $n, a > 1$ とする。 $a^n + 1$ が素数なら a は偶数で、ある自然数 m により $n = 2^m$ と書ける。

証明. a が奇数なら $a^n + 1$ は偶数。また、 $n = kl$ で l が奇数なら $a^{kl} + 1 = (a^k)^l + 1 = (a^k + 1)((a^k)^{l-1} - (a^k)^{l-2} + \cdots - a^k + 1)$ 。(l が偶数だとこういう分解はできないことに注意。) □

定義 3.6. $F_n = 2^{2^n} + 1$ を Fermat 数という。

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ は素数だが $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ は素数でない。そればかりか、 F_n が素数になる $n \geq 5$ は一つも知られていない。

命題 3.7. $n \neq m$ ならば F_n, F_m は互いに素。特に $\{p : \text{素数} \mid \text{ある } n \in \mathbb{N} \text{ について } p|F_n\}$ は無限集合。これから素数が無限にあることも従う。

証明. $n > m$ とする。 $F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = F_{n-1}(F_{n-1} - 2) = \cdots = F_{n-1}F_{n-2} \cdots F_m(F_{m-1} - 2)$ なので $p|F_n$ かつ $p|F_m$ なら $p|2$ となるが、定義から F_n は奇数。 □

次の定理はこの講義では証明できないが、興味深い話題なので紹介しておく：

定理 3.8 (Gauss). p を奇素数とする。正 p 角形が定規とコンパスだけで作図できるための必要十分条件は p が Fermat 数であること。

4. FERMAT の小品

この章では Fermat による次の二つの定理を取り上げる：

定理 4.1 (Fermat). (1) $y^2 = x^3 - 2$ の整数解は $(x, y) = (3, \pm 5)$ のみ。

(2) $y^2 = x^3 - 4$ の整数解は $(x, y) = (2, \pm 2), (5, \pm 11)$ のみ。

どちらも証明は意外なほど難しい。まずはもっと簡単な問題から見ていこう。

4.1. 素因数分解の一意性の活用.

命題 4.2. $y^2 - y = x^3$ の整数解は $(x, y) = (0, 0), (0, 1)$ のみ。

証明. $x, y \in \mathbb{Z}$ が $y(y-1) = x^3$ を満たすと仮定する。鍵となる観察は次の二行にまとめられる：

y と $y-1$ の共通因子は $y - (y-1) = 1$ の因子でもあるので素数になり得ない。

従って、素因数分解の一意性により $y = a^3, y-1 = b^3$ ($a, b \in \mathbb{Z}$) と書ける。

$y = a^3 = b^3 + 1$ より $(a-b)(a^2 + ab + b^2) = 1$ で、 $a-b = a^2 + ab + b^2 = \pm 1$ を得る。 $a = b+1$ のときは $(b+1)^2 + (b+1)b + b^2 = 3b^2 + 3b + 1 = 1$ 、書き換えて $3b(b+1) = 0$ より $b = 0, -1$ 。 $a = b-1$ のときは $(b-1)^2 + (b-1)b + b^2 = 3b^2 - 3b + 1 = 1$ 、書き換えて $3b(b-1) = 0$ となり $b = 0, 1$ 。これから $y = 0, 1, 2$ を得る。あとは容易。□

例題 4.3. $y^2 = x^4 - x^3$ の整数解は $(x, y) = (1, 0), (0, 0)$ のみ。

いまの議論にひねりを加えると次の命題も証明できる。

命題 4.4 (Fermat). $x^4 + y^4 = z^2$ を満たす $x, y, z \in \mathbb{Z} \setminus \{0\}$ は存在しない。特に、 $n = 4$ のときは定理 1.1 が成立する。

証明. x, y, z が正整数となる解があると仮定し、その中で z が最小の解を取る。すると x, y, z は互いに素となる。 x, y の双方が偶数だと z も偶数となるので矛盾。 x, y の双方が奇数だと、左辺を 4 で割った余りが 2 となるが、右辺を 4 で割った余りは 0, 1 にしかなり得ないので矛盾。そこで x を奇数、 y を偶数（従って z は奇数）とする。

方程式を $y^4 = (z - x^2)(z + x^2)$ と書き直す。 $z - x^2$ と $z + x^2$ の共通因子は両者の和 $2z$ と差 $2x^2$ の因子でもあるから 2 しかあり得ない。 x, z は奇数なので

$$z - x^2 = 2a^4, z + x^2 = 8b^4 \quad (a, b \text{ は互いに素})$$

または

$$z - x^2 = 8b^4, z + x^2 = 2a^4 \quad (a, b \text{ は互いに素})$$

と書ける。第一の場合は $x^2 = -a^4 + 4b^4$ となり、4 で割った余りを見ると不可能と知れる。第二の場合を考える。まず、 $0 < a < z$ としてよく、 a は奇数であることに注意する。また、 $4b^4 = (a^2 - x)(a^2 + x)$ である。 $(a, x) = 1$ となることに注意すると、上の命題と同じ観察により $a^2 - x$ と $a^2 + x$ の共通因子は 2 のみであることが分かり、 $a^2 - x = 2c^4, a^2 + x = 2d^4$ と書くことができる。これより

$$a^2 = c^4 + d^4$$

を得る。これは z の最小性に反する。□

4.2. $\mathbb{Z}[\sqrt{-2}], \mathbb{Z}[i]$ における素因数分解の一意性の活用. はじめに挙げた Fermat の定理に戻り、 $y^2 = x^3 - 2$ の整数解を考えよう。 $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$ と書き直し、 $\mathbb{Z}[\sqrt{-2}]$ が「素因数分解の一意性」を満たすことを思い出す。あとで次の主張を示す：

$y + \sqrt{-2}, y - \sqrt{-2}$ の双方を割り切る $\mathbb{Z}[\sqrt{-2}]$ の元は単数に限る。

これが分かれば、($\mathbb{Z}[\sqrt{-2}]$ の単数は ± 1 に限ることを併せて用いると) ある整数 a, b によって $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ と書けることが分かる。右辺は $(a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$ と展開されるので、係数を比較して $(3a^2 - 2b^2)b = 1$ 、これから $b = \pm 1$ を、さらに $(a, b) = (\pm 1, 1)$ を、続いて $y = a^3 - 6ab^2 = \pm 5$ を、最後に $(x, y) = (3, \pm 5)$ を得る。

やり残した主張を示す。 y は奇数であることに注意する。実際、 y が偶数なら x も偶数だが、方程式の左辺は 4 で割り切れるのに右辺は割り切れないことになる。一方、 $y + \sqrt{-2}$ と $y - \sqrt{-2}$ の双方の ($\mathbb{Z}[\sqrt{-2}]$ における) 素因子は両者の差である $2\sqrt{-2} = -(\sqrt{-2})^3$ の因子でもあるから $\sqrt{-2}$ に限る。 $(\sqrt{-2}$ は $\mathbb{Z}[\sqrt{-2}]$ の素元。) ところが y は奇数なので、これは $y + \sqrt{-2}$ の約数たり得ない。□

例題 4.5. $y^2 = x^3 - 8$ の整数解 $(2, 0)$ のみであることを示せ。

同様に、 $x^3 = y^2 + 4 = (y + 2i)(y - 2i)$ と書き直し、 $\mathbb{Z}[i]$ における素因数分解の一意性を利用すると定理 4.1(2) が証明できる。 $\mathbb{Z}[i]$ の単数は $\pm 1, \pm i$ の四つあるので議論が若干面倒になることに注意せよ。

例題 4.6. 定理 4.1(2) に証明を与えよ。また、 $y^2 = x^3 - 9$ の整数解は存在しないことを示せ。

しかしながら、次の定理を示すことは容易ではない(この講義では証明を与えられない)：

定理 4.7. $y^2 = x^3 - 5$ の整数解は存在しない。

上と同じ方法が使えないのは、 $\mathbb{Z}[\sqrt{-5}]$ においては素因数分解の一意性が成り立っていないことによる。つまり、 $x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5})$ と変形しても $y + \sqrt{-5} = (a + b\sqrt{-5})^3$ のように書けると結論できない。より一般に、定数 $d \in \mathbb{Z}$ を固定したときに、方程式 $y^2 = x^3 + d$ の整数解を考えるという問題が考えられるが、これまでに観察したように d の値によって意外なほど難しさが変わってくる。これについてはこの講義の後半で立ち戻る。(解答を与えるわけではないが。)

注意 4.8. $n \geq 3, \zeta = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}$ とおく。Fermat の方程式 $x^n + y^n = z^n$ は

$$x^n = z^n - y^n = (z - y)(z - \zeta y)(z - \zeta^2 y) \cdots (z - \zeta^{n-1} y)$$

と書き換えることができる。ここで $0 \leq i < j \leq n - 1$ について $z - \zeta^i y, z - \zeta^j y$ の共通素因子がほとんどないことを示し、素因数分解の一意性を用いて $z - y = \alpha^n$ ($\alpha \in \mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{Z}\}$) と書ける、と推論することで Fermat 予想を解決しようという試みが、19世紀になされた。しかし(これまでの文脈から明らかなように)ほとんどの n において(例えば $n \geq 23$ が素数なら) $\mathbb{Z}[\zeta]$ という数の体系では、素因数分解の一意性が成り立たないため、この試みは失敗した。というよりは、むしろこの試みによって素因数分解の一意性が成り立つかどうかという重要な数論的問題が見いだされたともいえる。

4.3. 多項式類似. 命題 4.2 と同様にして次の命題が証明できる :

命題 4.9. $a \neq 0$ を定数とする. $Y(t)^2 = X(t)^3 + a$ となる多項式 $X(t), Y(t)$ は定数に限る.

証明. 「定数」と曖昧に書いているが、これは大きい範囲で考えればよりたくさんの解が見つかるはずである。従って、最も大きい「定数」である複素数 \mathbb{C} に対して証明しておけば実数や有理数の場合も証明されたことになる。すると平方根 $c = \sqrt{a}$ も自由に取れるので、かえって便利である。

$X^3 = (Y-c)(Y+c)$ と書き直す。 $Y-c, Y+c$ 双方の因子は両者の差である $2c$ の因子だから定数。これと $\mathbb{C}[t]$ が「素因数分解の一意性」を満たすことからある多項式 A, B により $Y-c = A^3, Y+c = B^3$ と書ける。(任意の単数 b が単数 d により $b = d^3$ と表せることを用いた。) $Y = A^3 + c = B^3 - c$ より $B^3 - A^3 = (B-A)(B^2 + BA + A^2) = 2c$ なので $B-A = u$ と $B^2 + BA + A^2$ は単数。 $B = A+u$ を代入すると、 $B^2 + BA + A^2 = (A+u)^2 + (A+u)A + A^2 = 3A^2 + 3uA + u^2$ となり、最高次の係数を見ると A が定数と知れる。 \square

例題 4.10. (1) $Y(t)^2 = X(t)^4 - X(t)^3$ を満たす多項式 X, Y は定数に限る。

(2) $c \neq 0$ を定数とする。 $Y(t)^2 = X(t)^5 + c$ を満たす多項式 X, Y は定数に限る。

しかし「 $Y(t)^2 = X(t)^3 + t$ となる多項式 X, Y をすべて求めよ」という問題になるとちょっとやりにくい。(\sqrt{t} は t の多項式ではないから。) これを一発で処理できる、強力な定理が ABC 定理。

注意 4.11. $n \geq 3, \zeta = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}$ とおく。 Fermat の方程式 $X(t)^n + Y(t)^n = Z(t)^n$ は

$$X^n = Z^n - Y^n = (Z - Y)(Z - \zeta Y)(Z - \zeta^2 Y) \cdots (Z - \zeta^{n-1} Y)$$

と書き換えることができる。ここで $0 \leq i < j \leq n-1$ について $Z - \zeta^i Y, Z - \zeta^j Y$ の共通素因子がほとんどないことを示し、素因数分解の一意性を用いて $Z(t) - Y(t) = A(t)^n$ ($A \in \mathbb{C}[t]$) と書ける、と推論することで Fermat 予想の多項式類似を解決しようという試みが、19世紀になされた。そして ($\mathbb{Z}[\zeta]$ の場合に反し、複素数 \mathbb{C} ははじめから ζ を元に持つので) $\mathbb{C}[t]$ においては素因数分解の一意性が成り立つため、この試みは成功した。とはいっても、これまでの例からみてこの方法による証明はかなり面倒な計算が必要になると想像できるであろう。われわれは別の議論によって Fermat 予想の多項式類似を証明する。

5. ABC 定理

この章では多項式の係数を \mathbb{R} としているが、 \mathbb{C} でも \mathbb{Q} でも [標数 0 の体なら] よい。

定義 5.1. $A \in \mathbb{R}[t] \setminus \{0\}$ の素元分解が $A = P_1^{e_1} \cdots P_r^{e_r}$ ($i \neq j$ なら P_i と P_j は同伴でない) であるとき、 $\text{rad } A = P_1 \cdots P_r$ と書く。これには単数倍の曖昧さが残るが、 $\deg \text{rad } A$ は曖昧さ無く定まる。

定理 5.2 (ABC 定理. Stothers 1981, Mason 1984). $A, B, C \in \mathbb{R}[t] \setminus \{0\}$ を、全てが定数ではない、互いに素な多項式で、さらに $A(t) + B(t) = C(t)$ を満たすものとする。(後半の等式から、 A, B が互いに素なら A, C も B, C も互いに素となる。) このとき、次が成り立つ:

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

この定理の証明は次の章で与える。

5.1. 定理 5.2 \Rightarrow 定理 1.3 の証明. $X(t)^n + Y(t)^n = Z(t)^n$ を満たす多項式 X, Y, Z があったとする。 $X(t), Y(t), Z(t)$ は互いに素と仮定してよい。この上で、 X, Y, Z がすべて定数の場合は「自明」の定義により排除される。そこで $A = X^n, B = Y^n, C = Z^n$ として ABC 定理が適用できて、

$$\max(\deg X^n, \deg Y^n, \deg Z^n) < \deg \text{rad}(X^n Y^n Z^n) = \deg \text{rad}(XYZ) \leq \deg(XYZ).$$

左辺は $n \deg X, n \deg Y, n \deg Z$ のどれに置き換えても成り立つ。その三式の和を取ると

$$n(\deg X + \deg Y + \deg Z) = n \deg(XYZ) < 3 \deg(XYZ).$$

$n \geq 3$ であったから $\deg(XYZ) = 0$ となり、 X, Y, Z のすべては定数でないことに矛盾する。 □

次の例題の (1) は命題 4.9 でも扱った。(2) はそのときに残した問題。

例題 5.3. (1) $Y^2 = X^3 + 1$ を満たす定数でない多項式の組 $(X(t), Y(t))$ は存在しないことを示せ。
 (2) $Y^2 = X^3 + t$ を満たす定数でない多項式の組 $(X(t), Y(t))$ は存在しないことを示せ。

あとでこの種の問題を系統的に扱うので、ここでは解答を述べないでおく。(系 10.7 を参照。)

例題 5.4. $X(t)^5 + Y(t)^5 = t^2 - 1$ を満たす多項式の組 (X, Y) は存在しないことを示せ。

解答 5.5. 存在したと仮定する。 X が定数だとすると $2 = \deg(t^2 - 1 - X^5) = \deg(Y^5) = 5 \deg(Y)$ となり矛盾。 Y についても同様で、 X, Y はどちらも定数でない。また、 X, Y が共通の素因子 P を持ったとすると $P^5 | (X^5 + Y^5) = t^2 - 1 = (t+1)(t-1)$ となり矛盾。従って $A = X^5, B = Y^5, C = t^2 + 1$ として ABC 定理を適用できて、

$$\begin{aligned} & \max(\deg(X^5), \deg(Y^5), \deg(t^2 - 1)) \\ & < \deg \text{rad}(X^5 Y^5 (t^2 - 1)) = \deg \text{rad}(XY(t^2 - 1)) \leq \deg(XY(t^2 - 1)) = \deg(XY) + 2, \end{aligned}$$

すなわち $5 \deg X \leq \deg(XY) + 1$ と $5 \deg Y \leq \deg(XY) + 1$ を得る。両辺を足すと $5 \deg(XY) \leq 2 \deg(XY) + 2$ 、整理して $3 \deg(XY) \leq 2$ となるが、 X, Y は定数でないから $\deg(XY) \geq 1$ なので矛盾。

例題 5.6. (難) $X^3 + Y^3 = 6t^2 + 2$ の解は $(X, Y) = (1+t, 1-t)$ と、その $(-1 \pm \sqrt{-3})/2$ 倍および (X, Y) の入れ替えに限ることを示せ。

6. ABC 定理の証明

6.1. 多項式の微分. ABC 定理の証明には「微分」の概念を必要とする。簡単に復習する。微分のことを知っていれば聞き流していいが、余裕のある人は次の点に注意してもらいたい：ここで扱う微分は完全に代数的な操作であり、「定数」が実数でなくても（従って極限操作が意味をなさない状況でも）通用する。（例えば \mathbb{R} を \mathbb{Q} で置き換えてもよい。もちろん \mathbb{C} でもよい。）

定義 6.1. $A(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ に対して $A'(t) = n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \dots + 2 a_2 t + a_1$ を $A(t)$ の微分と定義する。

この講義で必要な性質は以下の四つだけ： $A(t), B(t) \in \mathbb{R}[t]$ を多項式、 a, b を定数、 e を自然数とする。

- (1) $(aA(t) + bB(t))' = aA'(t) + bB'(t)$.
- (2) $A(t)$ が定数でなければ $\deg A'(t) = \deg A(t) - 1$. [以下で必要なのは $\deg A' < \deg A$ だけ.]
- (3) $A(t)^e | B(t)$ ならば $A(t)^{e-1} | B'(t)$.
- (4) $A(t)B'(t) = B(t)A'(t) \Leftrightarrow A(t) = cB(t)$, c : 単数. [これは正標数だと成り立たない.]

6.2. 証明. (1) と (2) は定義から直ちに分かる。(3) は次のように三段階に分けて証明できる：

(a) $[A(t)B(t)]' = A'(t)B(t) + A(t)B'(t)$. [$A = t^m, B = t^n$ のときは直接計算で分かる。(1) から $(A_1 B)' = A_1' B + A_1 B'$, $(A_2 B)' = A_2' B + A_2 B' \Rightarrow ((aA_1 + bA_2)B)' = (aA_1 + bA_2)'B = (aA_1 + bA_2)B'$ が分かる。 A, B を入れ替えたものも同様。これらを組み合わせると主張が従う。]

(b) $[A(t)^e]' = eA(t)^{e-1}A'(t)$. [(a) と帰納法]

(c) $[A(t)^e B(t)]' = A(t)^{e-1}[eA'(t)B(t) + A(t)B'(t)]$. [(a) と (b) を適用. これから (3) が従う.]

(4) の証明： \Leftarrow は容易。 \Rightarrow を示すには、 $A = P^e S, B = P^f T$ (P は素元、 S, T は P と互いに素) のとき $e = f$ を示せばよい。(c) より $AB' = P^{e+f-1}S(fP'T + PT')$, $A'B = P^{e+f-1}T(eP'S + PS')$ なので $S(fP'T + PT') = T(eP'S + PS')$ となる。従って $fP'ST, eP'ST$ は P で割った余りが一致する。 $P'ST$ は P と互いに素なので $e = f$ を得る。

[商の微分を用いれば： $AB' - BA' = 0 \Leftrightarrow (A/B)' = 0 \Leftrightarrow A/B = \text{定数}$.] □

6.3. ABC 定理の証明. $A, B, C \in \mathbb{R}[t]$ は互いに素で $A(t) + B(t) = C(t)$ を満たすとせよ。

(a) $D(t) := A(t)B'(t) - B(t)A'(t)$ とおくと $D = AC' - CA' = CB' - BC' \neq 0$ となる。

微分の性質 (1) を用いる。 $A + B = C$ より $A' + B' = C'$ なので、 $D = AB' - BA' = A(C' - A') - (C - A)A' = AC' - AA' - CA' + AA' = AC' - CA'$. 他も同様。最後の $\neq 0$ は微分の性質 (4).

(b) $\max(\deg A, \deg B, \deg C) + \deg(D) < \deg(ABC)$.

微分の性質 (2) より $\deg D \leq \deg(AB) - 1$, すなわち $\deg C + \deg D < \deg(ABC)$ を得る。(a) と対称性から左辺の C を A, B に置き換えたものも成り立つ。

(c) $A|D \text{ rad } A, B|D \text{ rad } B, C|D \text{ rad } C$.

(a) と対称性からはじめの式だけ示せばよい。 $A = aP_1^{e_1} \dots P_r^{e_r}$ を素元分解とする。 $i = 1, \dots, r$ に対し「 $P_i^{e_i} | D \text{ rad } A$ 」を示せばよい。 $\text{rad } A = P_1 \dots P_r$ だから、「 \dots 」は「 $P_i^{e_i-1} | D$ 」と同じ。 $D = AB' - A'B$ だから、「 \dots 」には「 $P_i^{e_i-1} | A$ と $P_i^{e_i-1} | A'$ 」を示せば十分。ところが、定義から $P_i^{e_i-1} | P_i^{e_i} | A$ であり、微分の性質 (3) より $P_i^{e_i-1} | A'$ も従う。

(d) $\deg(ABC) \leq \deg D + \deg \text{rad}(ABC)$.

A, B, C が互いに素であることに注意すれば (c) より $ABC | D \text{ rad}(ABC)$ を得る。この帰結。

(b) と (d) より、ABC 定理の証明が完結する。 □

7. abc 予想

7.1. はじめの予想. ABC 定理の整数での類似を考える。

- rad A の類似 : 整数 $a \neq 0$ の素因数分解が $a = \pm p_1^{e_1} \cdots p_r^{e_r}$ のとき、 $\text{rad } a = p_1 \cdots p_r$ とする。
- deg A の類似 : これは絶対値 $|a|$ に置き換える。(注意 2.3 を参照。)

ABC 定理で上の置き換えをすると次の主張になる : 「 $a, b, c \in \mathbb{Z} \setminus \{0\}$ が互いに素で $a + b = c$ ならば $\max(|a|, |b|, |c|) < \text{rad}(abc)$ が成り立つ?」 a, b, c は名前を付け替えれば全部正となり、 $a + b = c$ ならば $\max(|a|, |b|, |c|) = c$ である。互いに素な自然数の組 (a, b, c) で $a < b < c, a + b = c$ となるものを abc-triple と呼ぶ。

予想 7.1 (? abc 予想 1 ?). (a, b, c) が abc-triple ならば $c < \text{rad}(abc)$ が成り立つ?

しかし予想 7.1 は成り立たない。次のような反例がある :

$$\begin{array}{ll} 1 + 8 = 9 & 9 > \text{rad}(1 \cdot 8 \cdot 9) = 2 \cdot 3 = 6 \\ 5 + 27 = 32 & 32 > \text{rad}(5 \cdot 27 \cdot 32) = 5 \cdot 3 \cdot 2 = 30 \end{array}$$

ただし、反例のある「割合」はかなり少ない :

- abc-triple で $c < 10000$ なるものは約 $1.5 \cdot 10^7$ 個あり、そのうち反例は 120 個。
- abc-triple で $c < 50000$ なるものは約 $3.8 \cdot 10^8$ 個あり、そのうち反例は 276 個。

そこで、予想 7.1 は正しくなくてもいい線いっているように見える。小さい修正を施してみる。はじめに思いつくのは、適当な定数 M を取って右辺の $\text{rad}(abc)$ を $M \text{rad}(abc)$ に置き換えることだが :

例題 7.2. $r = 1, 2, \dots$ に対し $(a, b, c) = (1, 3^{2^r} - 1, 3^{2^r})$ とおくと、 $\text{rad}(abc)/c$ は必ず 1 より小さく (つまり予想 7.1 の反例で) , しかもこの値は任意に小さくなることを示せ。

証明. $r \geq 1$ のとき $3^{2^r} - 1 = (3^{2^{r-1}})^2 - 1 = (3^{2^{r-1}} + 1)(3^{2^{r-1}} - 1) = \cdots = (3^{2^{r-1}} + 1)(3^{2^{r-2}} + 1) \cdots (3 + 1)(3 - 1)$ であり、 (\cdots) はすべて偶数である上に、最後の $3 + 1 = 4$ に注目すれば $2^{r+2} | 3^{2^r} - 1$. 従って $\text{rad}(abc) = \text{rad}((3^{2^r} - 1)3^{2^r}) \leq \frac{3^{2^r} - 1}{2^{r+1}} \cdot 3 < \frac{3}{2^{r+1}} c$. \square

だから、上のもくろみは (どんなに大きい M を取っても) 成り立たないことが分かる。そこで :

予想 7.3 (abc 予想 2). (a, b, c) が abc-triple ならば $c < [\text{rad}(abc)]^2$ が成り立つ?

この予想は未解決である。つまり、証明も反例も見つかっていない。もしも正しければ、やはりフェルマー予想が証明できる :

?証明? 必要なら記号と符号を入れ替えて、正の整数 x, y, z が $x^n + y^n = z^n$ を満たすとせよ。(このとき $z > x, y$ に注意。) $a = x^n, b = y^n, c = z^n$ として予想を適用すると

$$z^n < \text{rad}(x^n y^n z^n)^2 = \text{rad}(xyz)^2 \leq (xyz)^2 < z^6.$$

$z > 1$ だから $n < 6$ が従う。 $n = 3, 4, 5$ の場合のフェルマー予想は (オイラー・フェルマー・ディリクレ?により) 知られているので、これで証明が完了する。 \square

7.2. 予想の改良. 予想 7.1 と 7.3 の中間の予想も考えられる。例えば、予想 7.3 を $c < [\text{rad}(abc)]^{1.7}$ に書き換えても反例は (証明も) 知られていない。しかし、1.6 まで下げると反例が三つ知られている：

$$(a, b, c) = (2, 3^{10} \cdot 109, 23^5), (11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23), (19 \cdot 1307, 7 \cdot 29^2 \cdot 31^9, 2^8 \cdot 3^{22} \cdot 5^4)$$

はじめの例では $c = \text{rad}(abc)^{1.62991\dots}$ であり、あとの二つでは指数はそれぞれ $1.62599\dots$, $1.62349\dots$ である [12]。指数を 1.5 まで下げると知られている反例は 13 個に増える。(1.4 だと 229 個。) 計算機を用いて相当大きい数まで探索してある ($c < 10^{20}$ となる abc-triple は確認済み) ので、次のように予想することもできるであろう (この予想も、証明も反例も知られていない)：

予想 7.4 (abc 予想 1.5). (a, b, c) が abc-triple ならば 13 個の例外を除き $c < [\text{rad}(abc)]^{1.5}$ が成り立つ？

7.3. 予想 7.4 の応用. 次の定理を予想したのは Catalan (1844)、証明したのは Mihăilescu (2002)[8]。

定理 7.5. $x^m - y^n = 1$ を満たす $x, y, m, n \in \mathbb{N}$ で $m, n \geq 2$ なるものは $3^2 - 2^3 = 1$ のみ。

予想 7.4 を仮定して定理 7.5 を証明することを試みる。定理にある x, y, m, n が存在したと仮定する。 $(a, b, c) = (1, y^n, x^m)$ として予想 7.3 を適用する。13 個の例外がこの形になっているかどうかはリストを見て簡単にチェックできる。そこで、予想 7.4 から $c < \text{rad}(abc)^{3/2}$ が成り立つと結論される。いま $x^m > y^n$ から $x^{m/n} > y$ となること注意して

$$x^m < \text{rad}(x^m y^n)^{3/2} = \text{rad}(xy)^{3/2} \leq (xy)^{3/2} < (x^{1+(m/n)})^{3/2} = x^{3(m+n)/2n}.$$

これより $m < 3(m+n)/2n$ で、書き換えると $2mn < 3m + 3n$ となる。 $m, n \geq 2$ に注意すると $3n > (2n-3)m \geq (2n-3)2 = 4n-6$ 、すなわち $n < 6$ を得る。同様に $m < 6$ も成り立つ。こうして、考察すべき (m, n) は有限個におさまった。それぞれについて、実際に解を決定することも易しくはないが、もとの問題の難しさは (Fermat 予想と同じように) m, n の範囲が無数にあるという点にあった。それがこのように有限の範囲に収まってしまえば、あとは何とかやりようもある。

もう少し計算を進めてみると、 $m \geq 3$ となるのは $n = 2$ に限ることが分かる。実際、 $m \geq 3$ なら不等式 $2mn < 3m + 3n$ より $3n > (2n-3)m \geq 6n-9$ 、すなわち $n < 3$ を得る。 m, n を入れ替えても同じなので、結局、 m, n のどちらかは必ず 2 となる。さらに $m, n < 6$ だったから、 $(m, n) = (2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (4, 2), (5, 2)$ の 7 個の可能性しかないことが分かった。 $m = 2$ のときは $x^2 - y^n = 1$ を $y^n = (x+1)(x-1)$ と書き換えて、 $n = 2$ のときは $x^m - y^2 = 1$ を $x^m = (y+i)(y-i)$ と書き換えて、素因数分解の一意性を用いた (定理 4.1 と同様の) 議論によって解を洗い出すことができる。実行するのはたいへんだし、そもそも予想 7.4 は正しいと保証できていないのだが、もしも予想 7.4 を証明できれば Catalan 予想の別証明が得られるということは確かである。

7.4. 最終的な予想. Joseph Oesterlé と David Masser は 1985 年に次の予想を提出した：

予想 7.6 (abc 予想). 任意の $\kappa > 1$ に対し $c < [\text{rad}(abc)]^\kappa$ を満たさない abc-triple (a, b, c) は有限個。

もちろん未解決の問題である。ここで、 $\kappa \geq 1$ に対して abc 例外リストを次のように定義しよう：

$$\text{abc}[\kappa] := \{(a, b, c) \mid a < b < c, a + b = c, a, b, c \text{ は互いに素}, c < \text{rad}(abc)^\kappa\}.$$

$\text{abc}[2]$ は空であるというのが予想 7.3 で、 $\text{abc}[1.5]$ は既知の 13 個の元だけからなる、というのが予想 7.4 であった。予想 7.6 は任意の $\kappa > 1$ に対して $\text{abc}[\kappa]$ は有限集合ということを述べているが、もう少し強く、 $\kappa > 1$ を固定したら $\text{abc}[\kappa]$ の元をすべてリストアップできる、と解釈しておこう。なお、例題 7.2 によって $\text{abc}[1]$ は無限集合である。

8. abc 予想の応用

8.1. フェルマー予想の拡張. 次の定理は定理 1.1 の拡張.

定理 8.1. p, q, r を自然数で $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ を満たすようなものとする. 予想 7.6 が成り立つなら、互いに素な正の整数 x, y, z で $x^p + y^q = z^r$ を満たすものは、abc 例外リスト $abc[\kappa]$ から定まる有限個しか存在しない. ここで κ は $1 < \kappa < (\frac{1}{p} + \frac{1}{q} + \frac{1}{r})^{-1}$ なる任意の実数.

証明. (a) κ を $1 < \kappa < (\frac{1}{p} + \frac{1}{q} + \frac{1}{r})^{-1}$ となるように選び、予想 7.6 を κ に対して適用する: $abc[\kappa]$ にリストアップされている有限個の例外を除き、 $a + b = c$ となる互いに素な (a, b, c) は次を満たす:

$$\max(a, b, c) < \text{rad}(abc)^\kappa.$$

(b) 定理にある x, y, z をとる. (a) に $a = x^p, b = y^q, c = z^r$ を代入する. x, y, z は正なので、左辺は $c = z^r$ に一致する. 右辺は $\text{rad}(x^p y^q z^r)^\kappa = (xyz)^\kappa$ であるが、 $a = x^p < c = z^r, b = y^q < c = z^r$ なので

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

(c) これより

$$r < \kappa\left(\frac{r}{p} + \frac{r}{q} + 1\right), \quad \text{すなわち} \quad 1 < \kappa\left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right).$$

これは κ の選び方に反する. これで $(a, b, c) = (x^p, y^q, z^r) \in abc[\kappa]$ が示された. □

注意 8.2. • この定理は abc 予想を仮定しない証明が知られている [3]. さらに、非自明な解は次で尽くされると予想されている:

$$\begin{aligned} 1^n + 2^3 &= 3^2, & 2^5 + 7^2 &= 3^4, & 7^3 + 13^2 &= 2^9, & 2^7 + 17^3 &= 71^2, & 3^5 + 11^4 &= 122^2, \\ 17^7 + 76271^3 &= 21063928^2, & 1414^3 + 2213459^2 &= 65^7, & 9262^3 + 15312283^2 &= 113^7, \\ 43^8 + 96222^3 &= 30042907^2, & 33^8 + 1549034^2 &= 15613^3. \end{aligned}$$

Darmon [2] はこの他の反例を発見した者にカナダドルで次の額の賞金を与えると述べている:

$$300\left(\frac{1}{\frac{1}{p} + \frac{1}{q} + \frac{1}{r}} - 1\right).$$

- $p, q, r \geq 3$ のとき「有限」を「存在しない」に置き換えた主張が成り立つか、という問題には十万ドルの賞金がかかっている。(Beal/Tijdeman-Zagier 予想.) もちろん、これは上で述べた Darmon の懸賞問題 (とフェルマー予想の $n = 3$ の場合) から従う.
- $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ なら $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1 - \frac{1}{42}$ で、等号が成り立つのは $(p, q, r) = (2, 3, 7)$ の置換のみ. したがって、定理において abc 例外リストは $1 < \kappa < 42/41$ となる κ について考えれば十分.
- $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$ となる (p, q, r) は $(1, *, *)$, $(2, 2, *)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$ とその置換のみ.
- $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$ となる (p, q, r) は $(3, 3, 3)$, $(2, 4, 4)$, $(2, 3, 6)$ とその置換のみ.

8.2. Hall の予想. 定理 4.1 を思い出そう。ここでは、 $\mathbb{Z}[\sqrt{-2}]$ や $\mathbb{Z}[i]$ における素因数分解の一意性を活用して、方程式 $y^2 = x^3 - 2$ や $y^2 = x^3 - 4$ の整数解をすべて決定したのであった。より一般に、 $d \in \mathbb{Z}$ を定数として $y^2 = x^3 + d$ の整数解を考えるのは自然であるが、 $d = -5$ の場合にすでに「 $\mathbb{Z}[\sqrt{-5}]$ は素因数分解の一意性を満たさない」という根源的な理由により行き詰まった。abc 予想が正しければ次の結果が得られる：

命題 8.3. $d \in \mathbb{Z} \setminus \{0\}$ とする。abc 予想が正しければ、 $y^2 = x^3 + d$ の整数解で、 x, y が互いに素となるものは有限個。

この命題は次の命題から直ちに従う：

命題 8.4. $0 < \epsilon < 1/2$ を満たす実数 ϵ を固定する。abc 予想が正しければ、abc 例外リスト $abc[6/(2\epsilon+5)]$ から定まる有限個の例外を除き、互いに素な $x, y \in \mathbb{Z}$ は $x^3 = y^2$ か $|x|^\epsilon < |x^3 - y^2|$ を満たす。

証明. $\kappa = 6/(2\epsilon + 5)$ とおくと、 $1 < \kappa < 6/5$ が成り立つ。 $[0 < \epsilon < 1/2 \Leftrightarrow 0 < 2\epsilon < 1 \Leftrightarrow 5 < 2\epsilon + 5 < 6 \Leftrightarrow 6/5 > \kappa = 6/(2\epsilon + 5) > 1.]$ $d = x^3 - y^2 \neq 0$ として、この κ と $a = x^3, b = d, c = y^2$ に対して abc 予想を適用すると、 $abc[\kappa]$ に属する有限個の例外を除き

$$\begin{aligned} |x^3| < \text{rad}(dx^3y^2)^\kappa &\leq |dxy|^\kappa & \text{i.e.} & & |x|^{3-\kappa} < |d|^\kappa |y|^\kappa, \\ |y^2| < \text{rad}(dx^3y^2)^\kappa &\leq |dxy|^\kappa & \text{i.e.} & & |y|^{2-\kappa} < |dx|^\kappa, \quad |y| < |dx|^{\frac{\kappa}{2-\kappa}} \end{aligned}$$

を得る。 $|y|$ を消去して

$$|x|^{3-\kappa} < |d|^\kappa |dx|^\kappa \frac{\kappa}{2-\kappa} = |d|^{\frac{2\kappa-\kappa^2+\kappa^2}{2-\kappa}} |x|^{\frac{\kappa^2}{2-\kappa}} = |d|^{\frac{2\kappa}{2-\kappa}} |x|^{\frac{\kappa^2}{2-\kappa}},$$

となる。これより $|x|^{3-\kappa-\frac{\kappa^2}{2-\kappa}} = |x|^{\frac{(3-\kappa)(2-\kappa)-\kappa^2}{2-\kappa}} = |x|^{\frac{6-5\kappa}{2-\kappa}} < |d|^{\frac{2\kappa}{2-\kappa}}$ を得る。あとは指数だけを見ると、 $\frac{6-5\kappa}{2-\kappa} \cdot \frac{2-\kappa}{2\kappa} = \frac{6-5\kappa}{2\kappa} = (6 - 5 \cdot 6/(2\epsilon + 5))/(2 \cdot 6/(2\epsilon + 5)) = (12\epsilon + 30 - 30)/12 = \epsilon$ で証明完了。□

注意 8.5. (1) 命題 8.3 は命題 8.4 から直ちに従うが、逆はまったく成り立たない。つまり、命題 8.4 は命題 8.3 よりもはるかに強い。命題 8.4 では解の存在する x の範囲まで分かってしまうが、命題 8.3 ではそれが分からないというのが違いである。命題 8.4 は ($|x|^\epsilon < |d|$ の範囲の x すべてと、abc 例外リスト $abc[6/(2\epsilon + 5)]$ をチェックすることにより) 解をすべて求める方法を与えているが、命題 8.3 はそれができない。

(2) Hall は abc 予想の仮定が無くても (さらに「互いに素」の仮定も無くても) 命題 8.4 が成り立つことを予想した。というよりはむしろ、Hall 予想は abc 予想のはしりであり、abc 予想は Hall 予想の一般化である。(Hall の論文は abc 予想よりもはるかに前の 1971 年に出版されている。) 2009 年現在、Hall 予想も未解決である。([6] を参照。)

(3) 命題 8.4 の多項式類似が Davenport の定理である。(定理 10.5、注意 10.6 を参照。)

(4) 命題 8.3 は abc 予想を仮定しない証明が知られている。(Mordell の定理。) さらに一般化された次の定理も知られている。(実際に Siegel が示した定理はこれよりさらに一般的である。)

定理 8.6 (Siegel, 1929). $a, b, c \in \mathbb{Z}$ を定数として $f(x) = x^3 + ax^2 + bx + c$ とおく。方程式 $f(x) = 0$ が重根をもたないならば、 $y^2 = f(x)$ を満たす整数の組 (x, y) は有限個。

例題 8.7. 命題 8.3 において「互いに素となる」という条件を外しても同じ結論が成り立つことを示せ。(ヒント： $y^2 = cx^3 + d$ という形の方程式をすべて考えて帰納法を使う。)

9. ERDÖS-WOODS の予想

この章はとばしてもよい。少し毛色の変った ABC 定理の別の応用と、その整数における類似を解説する。この章の内容は [4] によっている。

a が定数なら一次式 $t - a$ は素元である。逆に、次の定理が「代数学の基本定理」として知られている：

定理 9.1 (Gauss). $\mathbb{C}[t]$ の素元は、ある $a \in \mathbb{C}$ に対して一次式 $t - a$ と同伴である。

従って、任意のゼロでない多項式 $A(t) \in \mathbb{C}[t]$ は $A(t) = c \prod_{i=1}^n (t - a_i)^{e_i}$ ($c, a_i \in \mathbb{C}$, $e_i > 0$) と書かれる。このとき $\text{rad } A = \prod (t - a_i)$ である。この次数 $\deg \text{rad } A$ は A の相異なる根の (重複をこめないで数えた) 個数と解釈することができる。この解釈はたいへん便利である。

命題 9.2. $X(t), Y(t) \in \mathbb{C}[t]$ を定数でない多項式とする。 $X(t)$ と $Y(t)$ は共通の根を持ち、 $X(t) + 1$ と $Y(t) + 1$ も共通の根を持つならば $X(t) = Y(t)$ であることを示せ。

証明. $\deg X \geq \deg Y$ と仮定してよい。

(a) $(A, B, C) = (X, 1, X + 1)$ に ABC 定理を適用すると $\deg X < \deg \text{rad}(X(X + 1))$ を得る。

(b) $\text{rad}(X(X + 1)) \mid \text{rad}(X - Y)$ を示す。上の注意から、これは「 $X(X + 1)$ の根は $X - Y$ の根である」ことを意味する。仮定から X の根は Y の根であり、従って $X - Y$ の根。同様に $X + 1$ の根は $Y + 1$ の根であり、従って $(X + 1) - (Y + 1) = X - Y$ の根。これを合わせると主張が従う。

(a), (b) より、 $X = Y$ でない限り $\deg X < \deg \text{rad}(X - Y) \leq \deg(X - Y) \leq \deg X$ となり矛盾。 \square

命題 9.2 の整数類似を考えると次のようになる：

整数 $a, b > 1$ が $\text{rad } a = \text{rad } b$, $\text{rad}(a + 1) = \text{rad}(b + 1)$ を満たすならば $a = b$ か？

答えは否である。またしても abc-triple $(1, 8, 9)$ が反例 $a = 2, b = 8$ を与える。反例の無限列 $(a, b) = (2^k - 2, 2^k(2^k - 2))$ ($k = 2, 3, \dots$) もある。しかし、少し変更した次の予想は未解決問題：

予想 9.3 (Erdős-Woods). 十分大きい $k \in \mathbb{N}$ に対し、次の集合は空であろう：

$$\{(a, b) \mid a, b \in \mathbb{N}, a \neq b, \text{rad}(a + i) = \text{rad}(b + i) \ (i = 0, 1, \dots, k)\}.$$

Langevin は、abc 予想が真ならこの予想は ($k = 3$ で、有限個の例外を除き) 正しいことを示した。

10. ABC 定理の応用

abc 予想が整数に関して多くの結果をもたらすことを見てきた。この章では、ABC 定理を用いると多項式に関して類似の結果が得られることを見る。

10.1. Catalan 予想の類似. 次は Catalan 予想 (定理 7.5) の類似であり、例題 5.3 の拡張とも見なせる。($(m, n) = (3, 2)$ の場合が例題 5.3 である。)

例題 10.1. ABC 定理を用いて次の定理を示せ :

$m, n \geq 2$ のとき、 $X(t)^m - Y(t)^n = 1$ を満たす定数でない多項式 $X(t), Y(t)$ は存在しない。

解答 10.2. 両方が定数ではない多項式 $X(t), Y(t)$ で $X^m - Y^n = 1$ を満たすものと仮定する。

$A = 1, B = Y^n, C = X^m$ として ABC を適用すると

$$\max(m \deg X, n \deg Y, 0) < \deg \text{rad}(X^m Y^n) = \deg \text{rad}(XY) \leq \deg(XY).$$

つまり

$$m \deg X < \deg(XY), \quad n \deg Y < \deg(XY).$$

(第一式) $\times n +$ (第二式) $\times m$ を書くと

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

X, Y の双方が定数ではないから $mn < m + n$ 、すなわち $(m - 1)(n - 1) < 1$ を得る。

10.2. フェルマー予想の拡張の類似. 次の例題は定理 8.1 の類似であり、定理 1.3 の拡張 :

例題 10.3. 自然数 p, q, r が $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$ を満たすとき、 $X^p + Y^q = Z^r$ を満たす定数でなく互いに素な多項式は存在しないことを示せ。

解答 10.4. $A = X^p, B = Y^q, C = Z^r$ として ABC 定理を適用すると

$$\max(\deg(x^p), \deg(Y^q), \deg(Z^r)) < \deg \text{rad}(X^p Y^q Z^r) = \deg \text{rad}(XYZ) \leq \deg(XYZ)$$

すなわち $p \deg X < \deg(XYZ), q \deg Y < \deg(XYZ), r \deg Z < \deg(XYZ)$ を得る。これから $\deg(XYZ) < (\frac{1}{p} + \frac{1}{q} + \frac{1}{r}) \deg(XYZ)$ で、 X, Y, Z がすべて定数でない限り仮定に反す。

10.3. Davenport の定理. 定理 4.1, 8.3 では $d \in \mathbb{Z} \setminus \{0\}$ として $y^2 = x^3 + d$ の整数解を考察した。以下ではこの多項式類似、すなわち多項式 $D(t) \neq 0$ を固定したとき、 $Y(t)^2 = X(t)^3 + D(t)$ を満たす多項式の組 $(X(t), Y(t))$ を求める、という問題を考える。次の定理は Hall 予想 8.4 の類似。

定理 10.5 (Davenport). X, Y が互いに素な定数でない多項式で $X^3 \neq Y^2$ ならば次が成り立つ：

$$\deg X \leq 2(\deg(X^3 - Y^2) - 1), \quad \deg Y \leq 3(\deg(X^3 - Y^2) - 1).$$

証明. $A = X^3, B = -Y^2, C = X^3 - Y^2$ として ABC 定理を適用すると

$$3 \deg X \leq \deg \text{rad}(XYC) - 1 \leq \deg(XYC) - 1, \quad \text{i.e.} \quad 2 \deg X \leq \deg Y + \deg C - 1,$$

$$2 \deg Y \leq \deg \text{rad}(XYC) - 1 \leq \deg(XYC) - 1, \quad \text{i.e.} \quad \deg Y \leq \deg X + \deg C - 1$$

を得る。これらから $\deg X, \deg Y$ を消去した式が求める式。 \square

注意 10.6. Davenport は、定理 10.5 において X, Y が互いに素でなくとも $X^3 \neq Y^2$ なら同じ式が成り立つことを示した。[9] を参照。

Davenport の定理によれば、 $Y^2 = X^3 + D$ の多項式解を探すには $\deg X \leq 2(\deg D - 1)$, $\deg Y \leq 3(\deg D - 1)$ の範囲だけを探索せばよいということになる。 X, Y の次数に上限ができてしまうのだから探索の範囲が（いわば「有限の範囲」に）狭まっている訳で、これはたいへん強力な定理である。例えば、すぐに次が分かる（例題 5.3 を参照）：

系 10.7. $D \neq 0$ が定数か一次式ならば $Y^2 = X^3 + D$ の定数でない多項式解は存在しない。

証明. 定理 10.5 により X, Y の最大公約数 M が単数でないときのみを考えればよい。 Y^2, X^3 は M^2, M^3 で割り切れるが、 $\deg D \leq 1$ なので D は重複因子を持ち得ない。 \square

次に D が二次式の場合を考える。変換 $D(t) \mapsto aD(bt + c)$ ($a, b, c \in \mathbb{C}, ab \neq 0$) によって、 D が重複因子を持つなら $D(t) = t^2$ に、そうでないときは（例えば） $D(t) = 1 - 3t^2$ に変換できる。

命題 10.8. (1) $Y^2 = X^3 + t^2$ の多項式解は $(X, Y) = (0, \pm t)$ に限る。

(2) $Y^2 = X^3 + 1 - 3t^2$ の多項式解は $(X, Y) = (4t^2 - 1, 8t^3 - 3t)$, $(-1, \sqrt{-3}t)$ および、それらから変換 $(X, Y) \mapsto (\omega X, \pm Y)$ ($\omega^3 = 1$) で得られるものに限る。

証明. Davenport の定理を用いて丁寧に場合分けをする。はじめに X, Y に共通因子があるときを考える。(2) では D が重複因子を持たないからこういう解は無い。(1) では X, Y の共通因子は t に限る。 $X = tX_0, Y = tY_0$ とおいてもとの式に代入すると $Y_0^2 = tX_0^3 + 1$ となる。今度は $tX_0^3, Y_0^2, 1$ が互いに素となるので、どれかがゼロでない限りは ABC 定理が使えて

$$\max(1 + 3 \deg X_0, 2 \deg Y_0) \leq \deg X_0 + \deg Y_0$$

を得る。これから $2 + \deg X_0 + \deg Y_0 \leq 0$ が従い、矛盾。

次に X, Y が互いに素となる解を考える。Davenport の定理によって $\deg X \leq 2, \deg Y \leq 3$ となる。次数をみると起こりうるのは $(\deg X, \deg Y) = (2, 3), (0, 1)$ の二通りだけと分かる。まず $(\deg X, \deg Y) = (0, 1)$ の場合、 $X = a, Y = bt + c$ において代入すると

$$Y^2 = (bt + c)^2 = b^2t^2 + 2bct + c^2, \quad X^3 + D = a^3 + t^2 \text{ or } a^3 + 1 - 3t^2$$

を得る。係数を比較すると求める解を得る。

$(\deg X, \deg Y) = (2, 3)$ のケースは同じようにやると係数が増えてたいへんである。(1) では次のような工夫もできる： $X^3 = (Y + t)(Y - t)$ と書き直す。互いに素の仮定から、一次式 A, B により $Y + t = A^3, Y - t = B^3$ と書いて、ここから $2t = A^3 - B^3$ を得る。すると A, B, t は互いに素となる。ABC 定理から $3 = 3 \deg A < \deg A + \deg B + \deg(2t) = 3$ となり矛盾。

(2) をがんばって計算してみる。 $X = at^2 + bt + c, Y = dt^3 + et^2 + ft + g$ とおくと、

$$X^3 + 1 - 3t^2 = a^3t^6 + 3a^2bt^5 + 3(ab^2 + a^2c)t^4 + (6abc + b^3)t^3 + 3(b^2c + ac^2 - 1)t^2 + 3bc^2t + (c^3 + 1),$$

$$Y^2 = d^2t^6 + 2det^5 + (2df + e^2)t^4 + 2(dg + ef)t^3 + (2eg + f^2)t^2 + 2fgt + g^2.$$

この係数比較をするのだから手計算ではたまらないが、機械を使えばできるかもしれない。

別の方法を紹介する。 \mathbb{Z} から $\mathbb{Z}[i]$ や $\mathbb{Z}[\sqrt{-2}]$ に数の世界を広げたように、 $\mathbb{C}[t]$ から $\mathbb{C}[t, \sqrt{1-3t^2}] = \{A + B\sqrt{1-3t^2} \mid A, B \in \mathbb{C}[t]\}$ へと「多項式」の世界を広げるのである。この $\mathbb{C}[t, \sqrt{1-3t^2}]$ という世界でも「素因数分解の一意性」が成り立つ。数の世界の広げ方によっては（例えば $\mathbb{Z}[\sqrt{-5}]$ では）素因数分解の一意性が成り立たなくなったように、多項式の世界も広げ方によっては（例えば $\mathbb{C}[t, \sqrt{1-t^3}]$ では）素因数分解の一意性が成り立たなくなるので、これはまったく自明ではない事実である。ともかく、ここでは認めておこう。（後述の命題 10.9 を参照。）

この世界で、元の方程式を書き直すと $(Y + \sqrt{1-3t^2})(Y - \sqrt{1-3t^2}) = X^3$ となる。 $Y \pm \sqrt{1-3t^2}$ の双方の素因子があるとすれば $Y, \sqrt{1-3t^2}$ の因子であるが、後者の因子はそれ自身しかなく、すると Y は多項式だから $1-3t^2$ を因子に持つことになり、すると X, Y が互いに素という仮定に反する。したがって $Y \pm \sqrt{1-3t^2}$ は共通因子を持たない。素因数分解の一意性から $Y + \sqrt{1-3t^2} = (A + B\sqrt{1-3t^2})^3$ ($A, B \in \mathbb{C}[t]$) と書ける。右辺を展開すると $A(A^2 + 3B^2(1-3t^2)) + B(3A^2 + B^2(1-3t^2))\sqrt{1-3t^2}$ で、係数を比較して $B(3A^2 + B^2(1-3t^2)) = 1$ を得る。これから B が単数で、 $A = \pm Bt$ で、 $B^3 = 1$ となることが順々に分かる。これから $Y = A^3 + 3AB^2(1-3t^2) = \pm(3t - 8t^3)$ を得る。あとは容易。□

最後に補足。次の命題で $t \mapsto \sqrt{3t}$ と変数変換すれば上で必要だった主張となる：

命題 10.9. $\mathbb{C}[t, \sqrt{1-t^2}] = \{A(t) + B(t)\sqrt{1-t^2} \mid A, B \in \mathbb{C}[t]\}$ では素因数分解の一意性が成り立つ。

証明. $\mathbb{C}[w, \frac{1}{w}] = \{w^{-n}L(w) \mid L \in \mathbb{C}[w], n \in \mathbb{Z}\}$ は自然に定義された和・差・積を持つ集合である。 $\mathbb{C}[w]$ は素因数分解の一意性を持つので $\mathbb{C}[w, \frac{1}{w}]$ でも素因数分解の一意性が成り立つ。ただし、単数はゼロでない定数だけでなく、 cw^n ($c \neq 0 \in \mathbb{C}, n \in \mathbb{Z}$) という形の元全体に増える。

$t = i(1-w^2)/2w, w = \sqrt{1-t^2} + it$ という変数変換を考える。 $\sqrt{1-t^2} = (1 - (i(1-w^2)/2w)^2)^{1/2} = 1 + w^2, 1/w = 1/(\sqrt{1-t^2} + it) = \sqrt{1-t^2} - it$ だから、この変換は $\mathbb{C}[t, \sqrt{1-t^2}]$ と $\mathbb{C}[w, \frac{1}{w}]$ の元の間の変換を与える。さらに、次の計算から両者は逆変換であることが分かる：

$$i \frac{1-w^2}{2w} = i \frac{1 - (\sqrt{1-t^2} + it)^2}{2(\sqrt{1-t^2} + it)} = i \frac{1 - (1-t^2 + 2it\sqrt{1-t^2} - t^2)}{2(\sqrt{1-t^2} + it)} = \frac{2it(t - i\sqrt{1-t^2})}{2(\sqrt{1-t^2} + it)} = t,$$

$$\sqrt{1-t^2} + it = \sqrt{1 - (i \frac{1-w^2}{2w})^2} + i \cdot i \frac{1-w^2}{2w} = \sqrt{\frac{4w^2 + 1 - 2w^2 + w^4}{4w^2}} - \frac{1-w^2}{2w} = w.$$

つまり、この変換により $\mathbb{C}[t, \sqrt{1-t^2}]$ と $\mathbb{C}[w, \frac{1}{w}]$ は一対一に対応する。上で注意したとおり後者では素因数分解の一意性が成り立つので、前者でも成り立つ。□

注意 10.10. $\mathbb{C}[t, \sqrt{1-t^2}]$ において $1-t, 1+t, \sqrt{1-t^2}$ はどれも素元ではなく、二つの素元の積に分解される。例えば $1-t = \frac{1}{2}(i-it + \sqrt{1-t^2})(it-i + \sqrt{1-t^2})$ である。特に $(1-t)(1+t) = (\sqrt{1-t^2})^2$ の両辺のどちらも「素元分解」にはなっていない。

10.4. **Davenport-Stothers triple.** これまでの議論の延長線上にある研究結果をいくつか、証明抜きで紹介する。命題 10.8 で「一番面白い解」は (2) における $(X, Y) = (4t^2 - 1, 8t^3 - 3t)$ であろう。(他の解はなにか退化した解という感じがする。) これは (X, Y) 定理 10.5 の不等式において等号が成り立つ場合である。[10] に従い、この一般化として次の定義を導入する：互いに素な定数でない多項式の組 (X, Y, D) が

$$\deg X = 2m, \deg Y = 3m, \deg D = m + 1, Y^2 = X^3 + D$$

を満たすとき、位数 m の Davenport-Stothers triple (DSt) とよぶ。また、二つの DSt が変換 $(X, Y, D) \mapsto (a^2X(bt+c), a^3Y(bt+c), a^6D(bt+c))$ ($a, b, c \in \mathbb{C}, ab \neq 0$) で写りあうとき同値と定める。 (X, Y, D) が DSt とは (X, Y) は $Y^2 = X^3 + D$ の「一番面白い解」ということである。これまでの議論により、位数 1 の DSt は、同値を除き一つしか無いことが分かった。この場合ですらあんなに大変だったのだから、 $m > 1$ の場合をどのように扱っていいものが途方に暮れてしまうが、偉い人はいるもので、次のような定理が知られている：

定理 10.11 (Stothers [11]. [9, 10] も参照). 任意の $m \in \mathbb{N}$ に対して位数 m の DSt の同値類の個数 $St(m)$ は $1 \leq St(m) < \infty$ を満たす。さらに、 $St(m)$ を表す明示的な公式もある。特に $St(1) = St(2) = St(3) = St(4) = 1, St(5) = 4, St(6) = 6, St(7) = 19$.

- 位数 1 の DSt は上に挙げた $(4t^2 - 1, 8t^3 - 3t, -3t^2 + 1)$.
- 位数 2 の DSt は $(t^4 - 4t, t^6 - 6t^3 + 6, -8t^3 + 36)$.
- 位数 3 の DSt は $(t^6 + 4t^4 + 10t^2 + 6, t^9 + 6t^7 + 21t^5 + 35t^3 + \frac{63}{2}t, -(27t^4 + \frac{351}{4}t^2 + 216))$.
- 位数 4 はもう書ききれない。
- 位数 5 には有理数係数の多項式が二つ、 $\sqrt{-3}$ を係数に含むものが二つある。その一つは： $(t^{10} + 26t^8 + 7(34 + 3\sqrt{-3})t^6 + 24(35 + 18\sqrt{-3})t^4 + \frac{3}{2}(371 + 1509\sqrt{-3})t^2 + 3(-775 + 543\sqrt{-3}), \dots, \dots)$

最後に、次の定理を紹介してこの文章を終える。

定理 10.12. 任意の DSt に対し、それと同値な DSt (X, Y, D) で X, Y, D はどれも代数的数を係数とする多項式であるものがある。

代数的数とは有理数係数の多項式の根となる複素数をいう。例えば $\sqrt{2}$ は $t^2 - 2 = 0$ の根だから代数的数。同様に $\sqrt{-1}, \sqrt[3]{2}, \sqrt[4]{\sqrt[3]{4} + \sqrt{-5}}$ なども代数的。五次以上の方程式の根はこういう風に根号で表示できないが、それも (係数が有理数なら) 代数的。一方、 π や e は代数的でないことが知られている。複素数の中で代数的数は圧倒的に少ない。従って、上の定理は同じくらい圧倒的に非自明である。

[これは Belyi の定理から従う。実際、 (X, Y, D) が DSt のとき、有理関数 $u(t) = X(t)^3/D(t)$ は $\{0, 1, \infty\}$ の外で不分岐な被覆 $u: \mathbb{P}_t^1 \rightarrow \mathbb{P}_u^1$ を定めることが (Hurwitz の定理を用いると) 分かる。]

文献案内. このノートの作成には [1, 4, 5, 7] を大いに参考にした。ほとんどはインターネット上で入手できるので、ぜひ現物にあたってみてください。日本語で書かれたもので、インターネット上で入手できるものとしては [13] がある。ここでは Vojta 予想や Szpiro 予想にも触れられている。

REFERENCES

- [1] F. Beukers, The ABC-conjecture, (<http://www.math.leidenuniv.nl/~desmit/ic/abc/fritsABCpresentation.pdf> より入手可能.)
- [2] H. Darmon, Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation, C.R. Math. Rep. Acad. Sci. Canada Vol. 19 (1), 1997 pp. 3-14. (<http://www.math.mcgill.ca/darmon/pub/pub.html> より入手可能.)
- [3] H. Darmon and A. Granville, On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, Bull. London Math. Soc. 27 (1995), no. 6, 513-543. (<http://www.math.mcgill.ca/darmon/pub/pub.html> より入手可能.)
- [4] N. Elkies, The ABC's of Number Theory, The Harvard College Mathematics Review, 2007. (<http://www.thehcmr.org/main/issue1.1> より入手可能.)
- [5] A. Granville, T. Tucker, It's as easy as *abc*. Notices Amer. Math. Soc. 49 (2002), no. 10, 1224-1231. (<http://www.ams.org/notices/200210/> より入手可能.)
- [6] S. Lang, Old and new conjectured diophantine inequalities, Bull. Amer. Math. Soc. (N.S.) Volume 23, Number 1 (1990), 37-75. (<http://projecteuclid.org/handle/euclid.bams/1183555717> より入手可能.)
- [7] B. Mazur, Questions about powers of numbers. Notices Amer. Math. Soc. 47 (2000), no. 2, 195-202. (<http://www.ams.org/notices/200002/> より入手可能.)
- [8] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture. J. Reine Angew. Math. 572 (2004), 167-195.
- [9] 塩田 徹治, *abc* 予想、楕円曲面、Mordell-Weil 格子, Lecture Notes in Mathematical Sciences 4, Univ. Tokyo, 2008. (<http://www.ms.u-tokyo.ac.jp/publication/documents/shellsurf3.pdf> より入手可能.)
- [10] T. Shioda, Elliptic surfaces and Davenport-Stothers triples. Comment. Math. Univ. St. Pauli 54 (2005), no. 1, 49-68 (<http://www.rkmath.rikkyo.ac.jp/math/shioda/> より入手可能.)
- [11] W. Stothers, Polynomial identities and Hauptmoduln. Quart. J. Math. Oxford Ser. (2) 32 (1981), no. 127, 349-370.
- [12] <http://www.math.unicaen.fr/~nitaj/abc.html>, <http://www.math.leidenuniv.nl/~desmit/abc/>
- [13] 田口 雄一郎, *abc* 予想の話, <http://www2.math.kyushu-u.ac.jp/~taguchi/nihongo/abc.html>
- [14] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443-551.

E-mail address: ytakao@math.tohoku.ac.jp