Hilbert の第 10 問題
Hilbert's Tenth Problem

y.*

2018 年 12 月 20 日

最終更新日: 2018 年 12 月 20 日

概要

多変数の多項式を用いて $f(x_1, \ldots, x_n) = 0$ の形で書ける代数方程式を Diophantus 方程式と呼ぶ．与えられた Diophantus 方程式が整数解 $(x_1, \ldots, x_n$ が全て整数であるような解) を持つか否かを判定する決定問題を Hilbert の第 10 問題という．本稿では MRDP 定理と呼ばれる定理の完全な証明を与え，その系として Hilbert の第 10 問題の決定不能性を示す．さらに，MRDP 定理以降のいくつかの結果も紹介する．本稿の大部分は MRDP 定理を証明した Matiyasevich 本人による教科書 [1] によっている．

Keywords: Hilbert の第 10 問題 (Hilbert's tenth problem), Diophantus 方程式 (Diophantine equation), Diophantus 的集合 (Diophantine set), c.e. 集合 (c.e. set), MRDP 定理 (MRDP theorem).

記号

本稿を通して，$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はそれぞれ自然数 (0 を含める)，整数，有理数，実数，複素数全体の集合を表す．

* http://iso.2022.jp/

目次

1 導入

ドイツの数学者 David Hilbert は 1900 年にパリで開かれた国際数学者会議において数学における 23 個の重要な未解決問題を提示した．そのうちの 10 番目の問題は次のようなものであった [2] [3]:

> n 個の未知数を含む整数係数の多項式 $P(x_1, x_2, \ldots, x_n)$ に対し，方程式 $P(x_1, x_2, \ldots, x_n) = 0$ (ディオファントス方程式または不定方程式と呼ぶ) が整数解を持つか否かを有限的に判定する方法をみつけよ．

Diophantus 方程式は数学において古くから研究されてきた素朴な対象である．例えば，有名な Fermat の最終定理は無限個の Diophantus 方程式

$$x^3 + y^3 - z^3 = 0, x^4 + y^4 - z^4 = 0, x^5 + y^5 - z^5 = 0, \ldots$$

がどれも $xyz = 0$ となるような自明な整数解しか持たない，すなわち x, y, z が全て正の整数となるような解はないということを主張している．Fermat の最終定理は Wiles と Taylor によって証明されたが，実際にはこのように解が全てわかっているような Diophantus 方程式はむしろ例外的である．例えば，

$$x^3 + y^3 + z^3 - 3 = 0 \tag{1}$$

という Diophantus 方程式が $(1, 1, 1), (4, 4, -5)$ とその並び換え以外の整数解を持つかどうかはわかっていない [2] [3].

1900 年当時はまだアルゴリズムというものの数学的な定式化がなされておらず，先程の問題文では「有限的に判定する方法」という数学的に曖昧な言い回しになっている．これを決定問題の形に書き直せば次のようになる．

問題 1.1 (Hilbert の第 10 問題 (Hilbert's tenth problem; HTP)).
Input: 有限変数の整数係数多項式 $f(x_1, \ldots, x_n) \in \bigcup_{k\in\mathbb{N}} \mathbb{Z}[x_1, \ldots, x_k]$
Question: Diophantus 方程式 $f(x_1, \ldots, x_n) = 0$ は整数解 $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ を持つか？

上では整数解の存否(そんぴ)を判定する問題を考えたが，解を考える範囲を整数環 $\mathbb{Z}$ から他の可換環 A に置き換えることで第 10 問題の様々な変種を考えることができる.[*1] A 内の解 $(x_1, \ldots, x_n) \in A^n$ の存否を判定する決定問題を $\mathrm{HTP}(A)$ と書くことにする．また，入力される多項式の変数の数 n や次数 d を制限した問題も考えることができる．入力を n 変数以下，d 次以下の多項式に制限した決定問題を $\mathrm{HTP}(A; n, d)$ と書くことにする．ただし，n や d に制限を設けないときは $n = \infty, d = \infty$ で表すことと約束しておく．したがって，この記法のもとでは元々の Hilbert の第 10 問題 1.1 は $\mathrm{HTP} = \mathrm{HTP}(\mathbb{Z}) = \mathrm{HTP}(\mathbb{Z}; \infty, \infty)$ と書けることになる．

注意 1.2. A 上の決定問題 $\mathrm{HTP}(A)$ について，入力される多項式の係数は基本的に A からとるものと考える．すなわち，入力は $\bigcup_{k\in\mathbb{N}} A[x_1, \ldots, x_k]$ の元であると思いたい．しかしながら，実際にはいくつかの理由からそうはできない場合がある:

[*1] 次節以降では主として $A = \mathbb{N}$ の場合を考えるので，実際には環ではなく (可換) **半環** (semiring) を考えていることになるのだが，いずれにせよ足し算と掛け算ができればよい．

- $A = \mathbb{N}$ のとき，HTP($\mathbb{N}$) の入力を自然数係数としてしまうと，「面白くない」問題になってしまう．実際，自然数係数多項式 $f(x_1, \ldots, x_n) \in \mathbb{N}[x_1, \ldots, x_n]$ を任意にとると，f の全ての係数が非負であることより $f(0, \ldots, 0)$ が f の最小値である．よって

$$f(x_1, \ldots, x_n) = 0 \text{ が自然数解 } (x_1, \ldots, x_n) \in \mathbb{N}^n \text{ を持つ } \iff f(0, \ldots, 0) = 0$$

  となってしまい，$(0, \ldots, 0)$ を代入するだけで解の存否がわかってしまうことになる．そこで，$A = \mathbb{N}$ のときは入力される多項式の係数は整数であるとする．すなわち，HTP($\mathbb{Z}$) の場合と同様に入力は $\bigcup_{k\in\mathbb{N}} \mathbb{Z}[x_1, \ldots x_k]$ からとる．ただし，実際には任意の整数係数多項式 $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ に対し，$f(x_1, \ldots, x_n) = 0$ という方程式は，係数が負の項を右辺へ移項することにより 2 つの自然数係数多項式 $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n) \in \mathbb{N}[x_1, \ldots, x_n]$ によって $f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n)$ という形の同値な方程式に変形できる (例えば方程式 (1) は明らかに $x^3 + y^3 + z^3 = 3$ という自然数係数の方程式と同値である)．だから入力の係数を変更するなどという大袈裟な言い方をせずとも，問題を少し変更して「2 つの自然数係数多項式 $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \bigcup_{k\in\mathbb{N}} \mathbb{N}[x_1, \ldots, x_k]$ に対し，$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ という形の Diophantus 方程式は自然数解を持つか？」とすれば済む程度の些細な問題ではある．
- $A = \mathbb{Q}$ や，より一般に $\mathbb{Z} \subseteq A \subseteq \mathbb{Q}$ のときは，入力の係数は A としても $\mathbb{Z}$ としてもよい．なぜなら，A 係数多項式 $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ があったときに，f の係数を全て既約分数の形に書いておいて，それらの分母の最小公倍数 l を掛けることで $l \cdot f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ とできるからである．
- $A = \mathbb{R}, \mathbb{C}$ の場合は状況が少し異なる．$A = \mathbb{N}$ の場合は問題が面白くない程度で済んだが，$A = \mathbb{R}, \mathbb{C}$ の場合には「Turing 機械では実数を扱うことができない」という本質的な問題が絡んでくる．このため，$A = \mathbb{R}, \mathbb{C}$ の場合には入力される係数の多項式は $\mathbb{Z}$ から，あるいは代数的実数 $\mathbb{R}_{\text{alg}} = \mathbb{R} \cap \overline{\mathbb{Q}}$ ないし代数的数 $\overline{\mathbb{Q}}$ からとるものと考える．[*2]決定問題とは入力に対し Yes/No を返す関数 $f\colon \Sigma^* \to \{\text{Yes}, \text{No}\}$ のことであったから，入力が Turing 機械で扱うことのできる形式になってさえいれば，「実数解 (または複素数解) が存在するか？」という問いは (Turing 機械で実数や複素数を厳密に扱うことができないという事実とは無関係に) 意味を持つということを注意しておく．

最後に，本稿のアウトラインを述べて本節を終えることにしよう．まず 2 節では HTP($\mathbb{Z}$) の決定不能性を HTP($\mathbb{N}$) の決定不能性に帰着する．次に 3 節で Diophantus 的集合という概念を定義し，それらの基本的な性質を調べる．また，Diophantus 的集合を組み合わせて新たな Diophantus 的集合を構成する方法を述べる．4 節では指数関数 $a = b^c$ が Diophantus 的関数であるという，Matiyasevich が証明した重要な定理の詳細な証明を与える．5 節では指数関数を縦横に用いて有限列のコード化の技法を開発する．6 節では c.e. 集合という計算可能性理論における概念を定義し，MRDP 定理の正確な主張を述べる．そして 7 節で Diophantus 方程式によって Turing 機械をシミュレートすることで HTP($\mathbb{N}$) の，したがって HTP($\mathbb{Z}$) の決定不能性を示す．最後に，8 節で Hilbert の第 10 問題の MRDP 定理以後の発展について触れて終わる．

[*2] 実数や複素数の場合と異なり，代数的数の計算・比較は計算機によって厳密に遂行することができる．詳細は例えば Cohen [4] や吉永 [5]，`@mod_poppo` [6] などを参照のこと．

2　整数解から自然数解へ

整数環 $\mathbb{Z}$ は自然数 $\mathbb{N}$ に比べると代数的には扱いやすいのだが，決定問題を考える上では符号による場合分けなどが発生してむしろ煩雑になることの方が多い．そのため，整数 $\mathbb{Z}$ に関する決定問題 HTP($\mathbb{Z}$) を自然数 $\mathbb{N}$ に関する決定問題 HTP($\mathbb{N}$) に翻訳しておくと，決定不能性の証明の見通しが良くなり，思考のリソースをいくらか節約することができる．本節では全ての作業を自然数 $\mathbb{N}$ 上で行うための下準備として，HTP($\mathbb{Z}$) の決定不能性が HTP($\mathbb{N}$) の決定不能性に帰着されることを見る．その鍵となる定理は次の Lagrange の四平方和定理である．

2.1　Lagrange の四平方和定理

ここでは整数解と自然数解の間の橋渡しをする Lagrange の四平方和定理を示す．念の為証明を載せておくが，色々な本に載っている有名な定理であるし (例えば [7, 定理 2.4.4])，結果だけ認めて証明は読み飛ばしてしまっても構わない．

定理 2.1 (Lagrange の四平方和定理 (Lagrange's four-square theorem) [1, Appendix 1]). どんな自然数 $n \in \mathbb{N}$ も，ある 4 つの整数 $x, y, z, w \in \mathbb{Z}$ によって $n = x^2 + y^2 + z^2 + w^2$ の形に書ける．

証明. まず，$n = 0, 1, 2$ に対しては定理は明らかに成り立つ．また簡単な計算により次の **Euler の四平方和恒等式** (Euler's four-square identity) が成り立つことが確かめられる:

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &\quad = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &\quad + (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned} \tag{2}$$

すなわち，整数の四平方和の積もまた四平方和である．このことから，n が奇素数の場合に定理を証明すれば十分であることがわかる．

p を任意の奇素数とする．2 つの数のリスト

$$r_0 := 0^2, \quad r_1 := 1^2, \quad \ldots, \quad r_i := i^2, \quad \ldots, \quad r_{(p-1)/2} := \left(\frac{p-1}{2}\right)^2, \tag{3.1}$$

$$l_0 := -1 - 0^2, \quad l_1 := -1 - 1^2, \quad \ldots, \quad l_i := -1 - i^2, \quad \ldots, \quad l_{(p-1)/2} := -1 - \left(\frac{p-1}{2}\right)^2 \tag{3.2}$$

を考える．これら 2 つのリスト (3.1)，(3.2) はともに次の性質を満たす:

$$\text{どの 2 つの要素も } p \text{ を法として互いに合同ではない.} \tag{4}$$

実際，$r_i \equiv r_j \pmod p$ とすると，$i^2 \equiv j^2 \pmod p$ だから $(i+j)(i-j) \equiv 0 \pmod p$ となる．p が素数であることより $\mathbb{Z}/p\mathbb{Z}$ は体，特に整域だから $i + j \equiv 0 \pmod p$ または $i - j \equiv 0 \pmod p$ であり，よって $i \equiv \pm j \pmod p$ である．一方，$0 \le i \le (p-1)/2$ かつ $0 \le j \le (p-1)/2$ だったから $0 \le i + j \le p - 1$ かつ $-(p-1)/2 \le i - j \le (p-1)/2$ である．したがって $i = j$ でなければならず，条件 (4) が成り立つことがわかる．(3.2) についても同様である．

2 つのリスト (3.1)，(3.2) は合計で $p+1$ 個の要素を持つから，鳩ノ巣原理より少なくともある 2 つの要素は p を法として互いに合同である．さらに，条件 (4) からその 2 つの要素はそれぞれ (3.1)，(3.2) から選ばれているはずである．ゆえにある i,j があって $r_i^2 \equiv l_j^2 \pmod{p}$，すなわち $i^2 \equiv -1 - j^2 \pmod{p}$ となる．よって i^2+j^2+1 は p で割り切れるので，ある自然数 $m \geq 1$ によって $i^2+j^2+1 = mp$ と書ける．すなわち，mp を $i^2+j^2+1^2+0^2 = mp$ と 4 つの平方数の和で書くことができた．今 $i,j \leq (p-1)/2$ だったから

$$\begin{aligned} mp &= i^2+j^2+1 \\ &\leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 \\ &= \frac{p^2-2p+3}{2} \\ &\leq \frac{p^2-2p+p}{2} \qquad (p \geq 3 \text{ より}) \\ &= \frac{p(p-1)}{2} < p(p-1) < p^2 \end{aligned}$$

となり，したがって $m < p$ でなければならない．

$m=1$ なら証明は終わりだから $m>1$ と仮定し，この m を小さくしていくことを考える．mp が 4 つの平方数の和で

$$x_1^2+x_2^2+x_3^2+x_4^2 = mp \tag{5}$$

と書けているとする．y_1,y_2,y_3,y_4 を

$$\begin{cases} y_i \equiv x_i \pmod{m}, \\ -m/2 < y_i \leq m/2 \end{cases} \qquad (i=1,2,3,4)$$

を満たすようにとる．このとき $y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m}$ だから，ある自然数 $m' \geq 0$ が存在して

$$y_1^2+y_2^2+y_3^2+y_4^2 = mm' \tag{6}$$

となる．$y_i \leq m/2$ であることを用いると $mm' = y_1^2+y_2^2+y_3^2+y_4^2 \leq (m/2)^2+(m/2)^2+(m/2)^2+(m/2)^2 = m^2$ だから $m' \leq m$ である．ここで等号が成立するのは $y_1=y_2=y_3=y_4=m/2$ のときだけであるが，$y_i \equiv x_i \pmod{m}$ を満たすためには $|x_i| \geq m/2$ でなければならない．よって (5) より $mp = x_1^2+x_2^2+x_3^2+x_4^2 \leq (m/2)^2+(m/2)^2+(m/2)^2+(m/2)^2 = m^2$ だから $p \leq m$ となるが，これは $m<p$ であったことに矛盾する．したがって $m' < m$ である．また $m' > 0$ であることもわかる．実際，仮に $m'=0$ とすると $y_1=y_2=y_3=y_4=0$ でなければならず，したがって $y_i \equiv x_i \pmod{m}$ から x_1,x_2,x_3,x_4 は全て m の倍数であるから (5) の両辺は m^2 で割り切れることになり，したがって p も m の倍数となる．ところが $1 \leq m < p$ だったから，これは p が素数であることに矛盾する．よって $0 < m' < m$ である．

以上より，(5) と (6) を辺々掛けて Euler の四平方和恒等式 (2) を適用すれば $m^2m'p$ が 4 つの平方数の和で

$$z_1^2+z_2^2+z_3^2+z_4^2 = m^2m'p \tag{7}$$

と書けることになる．ここで各 z_i は $y_i \equiv x_i \pmod{m}$ という条件から，m を法として

$$\begin{aligned} z_1 &= x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0, \quad ((5) \text{ より}) \\ z_2 &= x_1y_2-x_2y_1+x_3y_4-x_4y_3 \equiv 0, \\ z_3 &= x_1y_3-x_3y_1+x_2y_4-x_4y_2 \equiv 0, \\ z_4 &= x_1y_4-x_4y_1+x_2y_3-x_3y_2 \equiv 0 \end{aligned}$$

となる．すなわち，(7) の両辺は m^2 で割り切れる．したがって $m'p$ は 4 つの平方数の和で書ける．$0 < m' < m$ だったから，m' を改めて m と置いてこのプロセスを繰り返せばいずれ $m = 1$ となり，p が 4 つの平方数の和で書けることになる． □

2.2 整数解と自然数解の関係

ここでは先程示した Lagrange の四平方和定理を用いて，HTP($\mathbb{Z}$) と HTP($\mathbb{N}$) の関係を見る．帰着の一方は容易である:

補題 2.2. $n, d \in \mathbb{N} \cup \{\infty\}$ とする．HTP($\mathbb{Z}; n, d$) が決定不能ならば HTP($\mathbb{N}; 2n, d$) も決定不能である．

証明. $f(x_1, \ldots, x_n)$ を n 変数 d 次整数係数多項式とする．このとき

$$f(x_1, \ldots, x_n) = 0 \text{ が整数解を持つ} \iff f(x_1 - y_1, \ldots, x_n - y_n) = 0 \text{ が自然数解を持つ}$$

である． □

したがって特に HTP($\mathbb{Z}$) が決定不能ならば HTP($\mathbb{N}$) も決定不能である．

逆向きの帰着を示すために前小節で証明した Lagrange の四平方和定理を用いる．

補題 2.3. $n, d \in \mathbb{N} \cup \{\infty\}$ とする．HTP($\mathbb{N}; n, d$) が決定不能ならば HTP($\mathbb{Z}; 4n, 2d$) も決定不能である．

証明. $f(x_1, \ldots, x_n)$ を n 変数 d 次整数係数多項式とする．このとき Lagrange の四平方和定理 2.1 より

$$\begin{aligned} &f(x_1, \ldots, x_n) = 0 \text{ が自然数解を持つ} \\ \iff &f(x_1^2 + y_1^2 + z_1^2 + w_1^2, \ldots, x_n^2 + y_n^2 + z_n^2 + w_n^2) = 0 \text{ が整数解を持つ} \end{aligned}$$

である ($\Longrightarrow$ 向きに定理を使う). □

したがって特に HTP($\mathbb{N}$) が決定不能ならば HTP($\mathbb{Z}$) も決定不能である．

注意 2.4. 補題 2.2，2.3 の証明において，自然数の定義に 0 を含むかどうかは本質的ではない．実際，任意の整数 $k \in \mathbb{Z}$ に対し，k 以上の整数全体の集合を $\mathbb{Z}_{\geq k} := \{\, n \in \mathbb{Z} \mid n \geq k \,\}$ と書くことにすると，補題 2.2 は $\mathbb{N}$ を $\mathbb{Z}_{\geq k}$ に置き換えてもそのまま成り立つ．補題 2.3 については，証明中の $x_i^2 + y_i^2 + z_i^2 + w_i^2$ の代わりに $x_i^2 + y_i^2 + z_i^2 + w_i^2 + k$ を代入すればよい．

例 2.5. Fermat の最終定理の 3 次の場合の方程式

$$x^3 + y^3 - z^3 = 0$$

を考える．この方程式が正整数解を持たないということは，

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1)^3 + (y_1^2 + y_2^2 + y_3^2 + y_4^2 + 1)^3 - (z_1^2 + z_2^2 + z_3^2 + z_4^2 + 1)^3 = 0$$

という 12 変数の方程式が整数解を持たないことと同値である．

かくして補題 2.3 により，Hilbert の第 10 問題 HTP($\mathbb{Z}$) の決定不能性はいまや HTP($\mathbb{N}$) の決定不能性に帰着された．したがってこれ以降我々は全ての作業を自然数 $\mathbb{N}$ 上で行い，自然数解に関する理論の構築に注力することにする．

3　Diophantus 的集合の定義と性質

前節で述べたことから，現在の我々の最終目標は HTP($\mathbb{N}$) の決定不能性を示すことである．そのために，Turing 機械の停止問題を HTP($\mathbb{N}$) の中に見いだしたい．つまり，任意に与えられた Turing 機械 M に対して，対応する Diophantus 方程式 $f_M(x_1,\dots,x_{n(M)}) = 0$ を作りたい．一見すると Turing 機械の停止性と Diophantus 方程式の可解性との間には明らかな関係はないように見えるのだが，実はこの同値性の証明において中心的な役割を果たすのが本節で導入する Diophantus 的集合の概念である．

前節において今後の全ての作業を $\mathbb{N}$ の中で行うと述べたので，以降は特に断らない限り変数の動く範囲は $\mathbb{N}$ であるとする．

3.1　Diophantus 的集合

整数係数多項式 $f(a_1,\dots,a_n,x_1,\dots,x_m) \in \mathbb{Z}[a_1,\dots,a_n,x_1,\dots,x_m]$ を固定すると，自然数の n 個組 $(a_1,\dots,a_n) \in \mathbb{N}^n$ をひとつ決めるごとに $x_1,\dots,x_m$ を変数とする多項式 $f(a_1,\dots,a_n,x_1,\dots,x_m) \in \mathbb{Z}[x_1,\dots,x_m]$ ができ，[*3]したがって未知数 $x_1,\dots,x_m$ に関する Diophantus 方程式

$$f(a_1,\dots,a_n,x_1,\dots,x_m) = 0 \tag{8}$$

ができる．そして，パラメーター $(a_1,\dots,a_n)$ の値によって方程式 (8) が解を持つかどうかが定まる．方程式 (8) が解を持つようなパラメーター $(a_1,\dots,a_n)$ を集めた集合が Diophantus 的集合である．

定義 3.1 (Diophantus 的集合). $n > 0$ を正の整数とする．自然数の n 個組の集合 $D \subseteq \mathbb{N}^n$ が (n 次元の) **Diophantus 的集合** (Diophantine set) であるとは，ある自然数 $m \geq 0$ と整数係数の多項式 $f(a_1,\dots,a_n,x_1,\dots,x_m) \in \mathbb{Z}[a_1,\dots,a_n,x_1,\dots,x_m]$ が存在して

$$D = \{\, (a_1,\dots,a_n) \in \mathbb{N}^n \mid \exists (x_1,\dots,x_m) \in \mathbb{N}^m [f(a_1,\dots,a_n,x_1,\dots,x_m) = 0] \,\}$$

と書けることをいう．

3.3 節で様々な集合・関係・関数が Diophantus 的であることを示すので，ここでは非常に簡単な例を示すだけに留める．

例 3.2. 偶数全体の集合 $\mathrm{EVEN} = \{0,2,4,6,\dots\} \subseteq \mathbb{N}$，奇数全体の集合 $\mathrm{ODD} = \{1,3,5,7,\dots\} \subseteq \mathbb{N}$ は Diophantus 的である．実際，

$$\begin{aligned} \mathrm{EVEN} &= \{\, a \in \mathbb{N} \mid \exists x \in \mathbb{N}[a = 2x] \,\}, \\ \mathrm{ODD} &= \{\, a \in \mathbb{N} \mid \exists x \in \mathbb{N}[a = 2x+1] \,\} \end{aligned}$$

と書ける．

[*3] ここでは多項式の変数と，その変数に代入する自然数を同じ文字で書いている．これはあまりよい書き方ではないのだが，文字が足りなくなるのを回避するための苦肉の策でもある．これ以降も同様の書き方をするので，気になる読者は脳内で適切に別の記号を割り当ててほしい．

また，合成数全体の集合 $\mathrm{COMPOSITES} = \{4, 6, 8, 9, 10, 12, 14, \dots\} \subseteq \mathbb{N}$ も Diophantus 的である．実際，自然数 a が合成数であるのは，a が 2 以上の 2 つの自然数の積で書けるときだから，

$$f(a, x_1, x_2) := a - (x_1 + 2)(x_2 + 2)$$

とおけば

$$\mathrm{COMPOSITES} = \{\, a \in \mathbb{N} \mid \exists (x_1, x_2) \in \mathbb{N}^2 [f(a, x_1, x_2) = 0] \,\}$$

となる．

注意 3.3. Diophantus 的集合の定義には色々な見方がある．ここではそのような視点を 2 つだけ紹介する．

例えば，Diophantus 的集合とは多項式の零点集合の射影であると見ることができる．つまり，方程式 $f(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ によって定まる図形，つまりこの方程式を満たすような $n + m$ 次元空間内の点 $(a_1, \dots, a_n, x_1, \dots, x_m) \in \mathbb{N}^{n+m}$ を集めた集合を “$a_1, \dots, a_n$ 軸” に射影した集合とみなせる (図 1)．

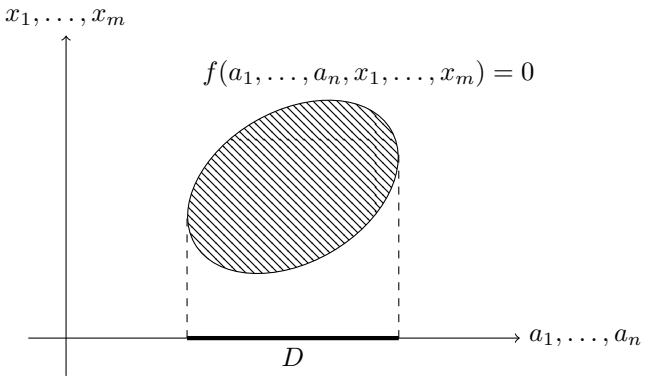


図 1: Diophantus 的集合は多項式の零点集合の射影である

また，Diophantus 的集合とは，多項式から決定問題を作る方法と思うこともできる．実際，多項式 $f(a_1, \dots, a_n, x_1, \dots, x_m)$ が与えられたとき，この多項式から定まる Diophantus 的集合 D は次の決定問題を表しているとみなせる．

> **Input:** パラメーター $(a_1, \dots, a_n) \in \mathbb{N}^n$
> **Question:** 未知数 $x_1, \dots, x_m$ に関する Diophantus 方程式 $f(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ は自然数解 $(x_1, \dots, x_m) \in \mathbb{N}^m$ を持つか？

さらに言い換えれば，Diophantus 的集合とは，$\mathrm{HTP}(\mathbb{N})$ の中から扱いやすい決定問題を “削り出す” ための手法であると思うことができる．

3.2 連立 Dipohantus 方程式

本節の最初で述べたように，$\mathrm{HTP}(\mathbb{N})$ の決定不能性を示すために Turing 機械から方程式への対応 $M \mapsto f_M(x_1, \dots, x_{n(M)})$ を構成したいのだが，これはそう簡単なことではない．簡単でないだけでなく，Turing 機械 M から一足飛びに巨大な Diophantus 方程式 $f_M(x_1, \dots, x_{n(M)}) = 0$ を作ってしまうと，M の停止性

と f_M の可解性との同値性の証明が非常に複雑なものになってしまい，何が本質なのかわからなくなってしまう上に汎用性のない結果になってしまう．証明の単純化と再利用性の向上を同時に達成するためには，Diophantus 方程式を単一の機能まで “分解” することが有効である．ここで導入する連立 Diophantus 方程式は Diophantus 方程式の “モジュール化” を実現し，単純な “部品” を組み合わせて複雑な方程式を構成することを可能にする．すなわち，「困難は分割せよ」である．

ここでは連立 Diphantus 方程式をひとつの Diophantus 方程式にまとめることができることを証明する．これはとても簡単な定理であるが，その簡単さに比べると重要性は非常に高い．ここでは $A = \mathbb{N}$ に限らず，もう少し一般の (半) 環 A に対して定理を証明する．

定理 3.4. $A \subseteq \mathbb{R}$ を部分 (半) 環とする．A 係数多項式 $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ に対し，[*4]連立 Diophantus 方程式

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \ldots, \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \tag{9}$$

が A に解を持つことと，Diophantus 方程式

$$f_1(x_1, \ldots, x_n)^2 + \cdots + f_m(x_1, \ldots, x_n)^2 = 0 \tag{10}$$

が A に解を持つことは同値である．

証明. 連立方程式 (9) の解が方程式 (10) の解でもあることは明らか．逆を示す．$A \subseteq \mathbb{R}$ という仮定から，A には $\mathbb{R}$ から定まる自然な順序構造が入っている．よって任意の $a \in A$ に対し $a^2 \geq 0$ となるので，等式 (10) が成り立つのは等式 (9) が成り立つ場合に限る． □

注意 3.5. ここでは「2 乗すると非負になる」という順序の性質を用いて定理 3.4 を証明をした．実は，環 A が順序環でなくても，A が整域で分数体 $\mathrm{Frac}(A)$ が代数閉体でなければ，連立 Diophantus 方程式をひとつの Diophantus 方程式にまとめることができる．証明は例えば Shlapentokh [8, Lemma 1.2.3] を参照のこと．

連立 Diophantus 方程式の簡単な応用として，4 次以下の Diophantus 方程式に関する第 10 問題 $\mathrm{HTP}(\mathbb{Z}; \infty, 4)$ の決定不能性がある．

系 3.6 (Skolem, 1938). $A \subseteq \mathbb{R}$ を部分 (半) 環とする．任意の A 係数 Diophantus 方程式は，等価な (つまり，解の存否が同値な) 4 次以下の Diophantus 方程式に変形できる (ただし，未知数の個数は増える)．特に，$\mathrm{HTP}(A)$ $(= \mathrm{HTP}(A; \infty, \infty))$ が決定不能ならば，入力を 4 次多項式に制限した $\mathrm{HTP}(A; \infty, 4)$ も決定不能である．

証明の概略. ここでは一般の場合の証明はせず，実例を挙げて説明するに留めるが，一般の場合でも全く同様である．未知数 x, y, z に関する Diophantus 方程式

$$4x^3y - 2x^2z^3 - 3xy^2 + 5z = 0 \tag{11}$$

を考える．このとき，方程式 (11) の可解性は次の $x, y, z, p_1, p_2, p_3, q_1, q_2, q_3, q_4, r_1, r_2$ を未知数とする連立

[*4] ただし，注意 1.2 の理由から，$A = \mathbb{N}$ など A が半環の場合には整数係数多項式を考えるものとする．これは系 3.6 においても同様である．

Diophantus 方程式の可解性と同値である:

$$\begin{cases} 4p_1 - 2q_1 - 3r_1 + 5z = 0, \\ p_1 = xp_2, \\ p_2 = xp_3, \\ p_3 = xy, \\ q_1 = xq_2, \\ q_2 = xq_3, \\ q_3 = zq_4, \\ q_4 = z^2, \\ r_1 = xr_2, \\ r_2 = y^2. \end{cases} \tag{12}$$

したがって，定理 3.4 の証明から，連立方程式 (12) の可解性は 12 変数の 4 次方程式

$$\begin{aligned}(4p_1 - 2q_1 - 3r_1 + 5z)^2 + (p_1 - xp_2)^2 + (p_2 - xp_3)^2 + (p_3 - xy)^2 \\ + (q_1 - xq_2)^2 + (q_2 - xq_3)^2 + (q_3 - zq_4)^2 + (q_4 - z^2)^2 + (r_1 - xr_2)^2 + (r_2 - y^2)^2 = 0\end{aligned}$$

の可解性と同値である．□

3.3 Diophantus 的関係・関数と Diophantus 的集合の閉包性

自然数 (の n 個組) の集合が Diophantus 的であることの定義は既に与えたが，ここでは関係や関数が Diophantus 的であることの定義を述べ，いくつかの基本的な関係や関数が実際に Diophantus 的であることを示す．さらに，Diophantus 集合のクラスが適切な**閉包性** (closure property) を持つことを証明する．標語的に言えば，複雑な Diophantus 的集合を作るための基本的な “部品” となる Diophantus 的集合と，それらを適切に “組み立てる” 方法を開発するということである．

まず，集合論における関係や関数に関する用語の定義を思い出しておこう．

定義 3.7. n **項関係** (n-ary relation) とは，部分集合 $R \subseteq \mathbb{N}^n$ のことである．R が n 項関係のとき，$(x_1, \ldots, x_n) \in R$ であることを $R(x_1, \ldots, x_n)$ で表す．n **項関数** (n-ary function) とは，$\mathbb{N}^n$ を定義域とする関数 $F\colon \mathbb{N}^n \to \mathbb{N}$ のことである．n 項関数 F の**グラフ** (graph) とは，$\mathbb{N}^{n+1}$ の部分集合 $\{\, (x_1, \ldots, x_n, F(x_1, \ldots, x_n)) \in \mathbb{N}^{n+1} \mid x_1, \ldots, x_n \in \mathbb{N} \,\}$ のことである．

n 項関係 R が Diophantus 的であるとは，R が集合として Diophantus 的集合であることをいう．n 項関数 F が Diophantus 的であるとは，F のグラフが Diophantus 的集合であることをいう．すなわち，「$F(x_1, \ldots, x_n) = x_{n+1}$」という $n+1$ 項関係が Diophantus 的であることをいう．

例 3.8. 次の関係は全て Diophantus 的である．[*5]

- 2 項関係 $a = b$ [*6]，
- 2 項関係 $a \neq b \iff \exists x[(a-b)^2 = x + 1]$，
- 2 項関係 $a \leq b \iff \exists x[a + x = b]$，

[*5] ここで $\exists x$ と書いてあるところは全て $\exists x \in \mathbb{N}$ の意味である (全ての作業を $\mathbb{N}$ 上で行っていたことを思い出そう)．

[*6] 実際，$f(a,b) := a - b$ とおけば，パラメーター a, b を決めるごとに未知数が 0 個の Diophantus 方程式 $f(a,b) = 0$ ができる．

- 2 項関係 $a < b \iff \exists x[a + x + 1 = b]$,
- 2 項関係 $a \mid b \iff \exists x[ax = b]$ (a は b を割り切る) [*7].

Diophantus 的関係を $\vee, \wedge, \exists$ などの論理結合子を用いて組み合わせることで，いくつかの Diophantus 的集合から別の Diophantus 的集合を “組み立てる” ことができる．つまり，Diophantus 的集合のなすクラスはこれらの論理演算について閉じている．

命題 3.9 (Diophantus 的集合の閉包性). $D_1, D_2, D \subseteq \mathbb{N}^n$ を n 次元の Diophantus 的集合とするとき，次の集合は全て Diophantus 的集合である．

1. 和集合 $D_1 \cup D_2$,
2. 共通部分 $D_1 \cap D_2$,
3. 各 i $(1 \leq i \leq n)$ に対し，第 i 軸に直交する超平面への D の射影
   $P_i := \{ (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \mathbb{N}^{n-1} \mid \exists y[(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n) \in D] \}$.

Diophantus 的関係の言葉で言い換えると，R_1, R_2, R が Diophantus 的な n 項関係であるとき，関係 $R_1(x_1, \ldots, x_n) \vee R_2(x_1, \ldots, x_n), R_1(x_1, \ldots, x_n) \wedge R_2(x_1, \ldots, x_n), \exists x_i R(x_1, \ldots, x_n)$ も Diophantus 的である．

証明. D_1, D_2, D を定義する多項式をそれぞれ

$$f_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}),$$
$$f_2(a_1, \ldots, a_n, y_1, \ldots, y_{m_2}),$$
$$f(a_1, \ldots, a_n, z_1, \ldots, z_m)$$

とおく．このとき，

1. $D_1 \cup D_2$ は $f_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) \cdot f_2(a_1, \ldots, a_n, y_1, \ldots, y_{m_2})$ で定義される．
2. $D_1 \cap D_2$ は $f_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1})^2 + f_2(a_1, \ldots, a_n, y_1, \ldots, y_{m_2})^2$ で定義される．[*8]
3. P_i は $f(a_1, \ldots, a_{i-1}, z_0, a_{i+1}, \ldots, a_n, z_1, \ldots, z_m)$ で定義される． □

注意 3.10. Diophantus 的集合 D の補集合 $\mathbb{N}^n \setminus D$ は一般には Diophantus 的集合**ではない**．すなわち，Diophantus 的関係 $R(x_1, \ldots, x_n)$ の否定 $\neg R(x_1, \ldots, x_n)$ は Diophantus 的であるとは限らない．このことは 7 節で証明する MRDP 定理の帰結の 1 つである．

系 3.11. $F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$ を Dipohantus 的関数とし，$R(y_1, \ldots, y_m)$ を Diophantus 的関係とする．このとき，合成関係

$$R(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n))$$

も Dipohantus 的である．特に，Diophantus 的関数の合成関数もまた Diophantus 的である．

証明. 仮定より m 項関係 $R(y_1, \ldots, y_m)$ と $n+1$ 項関係 $F_i(x_1, \ldots, x_n) = y_i$ $(1 \leq i \leq m)$ は Diphantus 的関

[*7] この定義のもとでは，全ての自然数が 0 を割り切り，また 0 は 0 のみを割り切ることに注意せよ．
[*8] $D_1 \cap D_2$ は $f_1 = 0, f_2 = 0$ という連立 Diophantus 方程式で定義できるので，定理 3.4 からと言ってもよい．

係だから，命題 3.9 より $m+n$ 項関係

$$R(y_1,\ldots,y_m) \wedge y_1 = F_1(x_1,\ldots,x_n) \wedge \cdots \wedge y_m = F_m(x_1,\ldots,x_n)$$

は Diophantus 的である．再び命題 3.9 より n 項関係

$$\exists y_1 \cdots \exists y_m [R(y_1,\ldots,y_m) \wedge y_1 = F_1(x_1,\ldots,x_n) \wedge \cdots \wedge y_m = F_m(x_1,\ldots,x_n)]$$

は Diophantus 的である．特に，R が関数のグラフから定まる関係の場合を考えれば，Diophantus 的関数の合成関数も Diophantus 的であることがわかる． □

命題 3.9，系 3.11 を用いると，様々な関係・関数が Diophantus 的であることを容易に示すことができる．

補題 3.12. 以下の関係・関数は全て Diophantus 的である．

1. $\max\{b-c,0\}$ を返す 2 項関数 $b \dot{-} c$,
2. 3 項関係 $a \mid (b-c)$, [*9]
3. b を $c \neq 0$ で割った余りを返す 2 項関数 $\mathrm{rem}(b,c)$,
4. $c \neq 0$ を法として b と合同な整数の絶対値の最小値を返す 2 項関数 $\mathrm{arem}(b,c)$ (図 2)
   (例えば，$\mathrm{arem}(5,7) = |-2| = 2$ である．また，常に $\mathrm{arem}(b,c) \leq c/2$ が成り立つ),
5. a が b を割り切らないことを表す 2 項関係 $a \nmid b$,
6. b を $c \neq 0$ で割った商 (小数部分は切り捨て) $\lfloor b/c \rfloor$ を返す 2 項関数 $b \operatorname{div} c$,
7. a と b が $c \neq 0$ を法として合同であることを表す 3 項関係 $a \equiv b \pmod{c}$,
8. b と c の最大公約数を返す 2 項関数 $\gcd(b,c)$,
9. b と c の最小公倍数を返す 2 項関数 $\mathrm{lcm}(b,c)$.

証明. 以下のようにすればよい．

1. $a = b \dot{-} c \iff (b \leq c \wedge a = 0) \vee (b > c \wedge a + c = b)$.
2. $a \mid (b-c) \iff a \mid (b \dot{-} c) \wedge a \mid (c \dot{-} b)$.
3. $a = \mathrm{rem}(b,c) \iff a < c \wedge c \mid (b-a)$ [*10].
4. $a = \mathrm{arem}(b,c) \iff 2a \leq c \wedge [c \mid (b-a) \vee c \mid (b+a)]$ $\quad (\iff 2a \leq c \wedge a \equiv \pm b \pmod{c})$.
5. $a \nmid b \iff \mathrm{rem}(b,a) > 0$.
6. $a = b \operatorname{div} c \iff ac + \mathrm{rem}(b,c) = b$ (剰余定理より).
7. $a \equiv b \pmod{c} \iff \mathrm{rem}(a,c) = \mathrm{rem}(b,c)$.
8. $a = \gcd(b,c) \iff bc > 0 \wedge a \mid b \wedge a \mid c \wedge \exists x \exists y [a + cy = bx]$
   ($a \mid b, a \mid c$ より $a \mid \gcd(b,c)$ であり，また $\gcd(b,c) \mid (bx - cy) = a$ だから).
9. $a = \mathrm{lcm}(b,c) \iff bc = a \gcd(b,c)$. □

[*9] 2 項関係 $a \mid b$ が Diophantus 的であるからといって $a \mid (b-c)$ が Diophantus 的関数であると直ちに結論してしまうのは早計である．実際，2 変数関数 $b-c$ は値が負になりうるので Diophantus 的関数ではなく，系 3.11 を適用することはできない．つまり，最終的にできあがる多項式は整数係数でもよいけれども，構成の途中で Diophantus 的関係・関数に負の数を代入してはいけないということである．

[*10] このように定義すると $c=0$ のときは対応する a が存在しないので厳密には $\mathrm{rem}(b,c)$ は Diophantus 的関数になっていないのだが，これ以降 $c \neq 0$ が保証される状況でしか使用しないので問題は発生しない．気になる読者は各自で $\mathrm{rem}(b,c) \iff (c = 0 \wedge a = 0) \vee (c \neq 0 \wedge a < c \wedge c \mid (b-a))$ のように書き直してほしい．他の関数についても同様である．

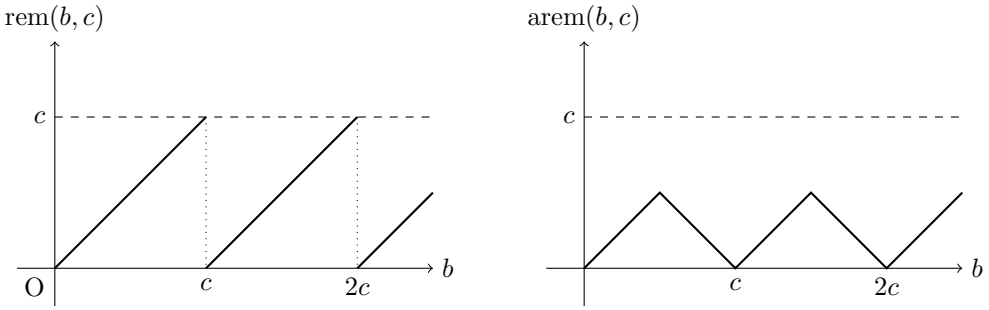


図 2: 法 c を固定したときの $\mathrm{rem}(b,c)$ と $\mathrm{arem}(b,c)$ の比較

4 指数関数は Diophantus 的である

1961 年までに Davis，Putnam，Robinson らの仕事によって「2 変数の指数関数 b^c が Diophantus 的関数ならば，Hilbert の第 10 問題は決定不能である」ということが示されていた [9, 7 章]．1970 年にこの最後のピースを埋め，Hilbert の第 10 問題の否定的解決を成し遂げたのが当時 22 歳のロシア (ソ連) の青年 Yuri V. Matiyasevich である．

本節では Matiyasevich 本人によって後に簡略化された証明に沿って指数関数 b^c が Diophantus 的であることを証明する [1, Section 2]．ただし，本節の証明は技術的で細かい議論が続くため，本稿を初めて読む際は本節の結果を認めてしまい，先に次節以降を読むことをお勧めする．

4.1 2 階線形回帰数列 $\alpha_b(n)$

ここでは指数関数 b^c が Diophantus 的であることを示す代わりに，技術的な理由から以下の数列 $\alpha_b(n)$ が b, n に関する Diophantus 的 2 項関数であることを示す．これは一見すると回りくどいことをしているように思うかもしれないが，実際には b^c が Diophantus 的であることを示すよりも $\alpha_b(c)$ が Diophantus 的であることを示す方がずっと簡単なのである．

定義 4.1. 自然数 $b \geq 2$ に対して，数列 $(\alpha_b(n))_{n=0}^{\infty}$ を次の漸化式で定義する:

$$\begin{aligned} \alpha_b(0) &:= 0, \\ \alpha_b(1) &:= 1, \\ \alpha_b(n+2) &:= b\alpha_b(n+1) - \alpha_b(n). \end{aligned}$$

最初の方のいくつかの項を書き下してみると，$\alpha_b(2) = b, \alpha_b(3) = b^2 - 1, \alpha_b(4) = b^3 - 2b, \ldots$ となる．

$\alpha_b(n)$ について簡単にわかる性質をいくつか述べておく．

補題 4.2. $\alpha_b(n)$ は狭義単調増加である:

$$\alpha_b(0) < \alpha_b(1) < \alpha_b(2) < \cdots.$$

よって特に，任意の n に対して $n \leq \alpha_b(n)$ である．

証明. $b \geq 2$ だったから，n に関する帰納法により $\alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) > b\alpha_b(n+1) - \alpha_b(n+1) = (b-1)\alpha_b(n+1) \geq \alpha_b(n+1)$. □

補題 4.3. α_2 は恒等写像である．すなわち，任意の n に対し

$$\alpha_2(n) = n.$$

証明. n に関する帰納法により $\alpha_2(n+2) = 2\alpha_2(n+1) - \alpha_2(n) = 2(n+1) - n = n+2$. □

一般に線形回帰数列は**コンパニオン行列** (companion matrix) を用いて書き表すことができる．今回の場合であれば

$$A_b := \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$$

とおくことによって

$$\begin{pmatrix} \alpha_b(n+2) \\ \alpha_b(n+1) \end{pmatrix} = A_b \begin{pmatrix} \alpha_b(n+1) \\ \alpha_b(n) \end{pmatrix}$$

と書ける．この A_b について次が成り立つ．

補題 4.4. 任意の $n \geq 0$ に対し

$$A_b^n = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

が成り立つ．ただし，$\alpha_b(-1) := -1$ と約束しておく．

証明. n に関する帰納法により

$$\begin{aligned} A_b^{n+1} &= \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \\ &= \begin{pmatrix} b\alpha_b(n+1) - \alpha_b(n) & -b\alpha_b(n) + \alpha_b(n-1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix}. \end{aligned}$$

□

A_b の行列式は $\det A_b = 1$ だから，$\det(A_b^{n+1}) = (\det A_b)^{n+1} = 1^{n+1} = 1$ である．よって補題 4.4 より

$$\begin{aligned} 1 = \det(A_b^{n+1}) &= -\alpha_b(n+2)\alpha_b(n) + \alpha_b(n+1)^2 \qquad (13) \\ &= -(b\alpha_b(n+1) - \alpha_b(n))\alpha_b(n) + \alpha_b(n+1)^2 \\ &= \alpha_b(n)^2 - b\alpha_b(n)\alpha_b(n+1) + \alpha_b(n+1)^2 \qquad (14) \end{aligned}$$

となる．これより次がわかる．

補題 4.5. 数列 $\alpha_b(n)$ の隣り合う 2 つの項は互いに素である．すなわち，任意の n に対し $\gcd(\alpha_b(n), \alpha_b(n+1)) = 1$ である．

証明. 初等整数論においてよく知られているように，2 つの自然数 x, y が互いに素であるためには

$$\exists u \in \mathbb{Z} \exists v \in \mathbb{Z}[ux + vy = 1]$$

となることが必要かつ十分である．よって式 (13) より $\alpha_b(n)$ と $\alpha_b(n+1)$ は互いに素である． □

また，式 (14) は次の補題の意味で数列 $\alpha_b(n)$ を特徴付けている．この著しい性質が b^c の代わりに $\alpha_b(c)$ を使う利点のひとつである．

補題 4.6. 2 つの自然数 $x, y \in \mathbb{N}$ が

1. $x \leq y$,
2. $x^2 - bxy + y^2 = 1$

を満たすならば，ある m について $x = \alpha_b(m), y = \alpha_b(m+1)$ となる．

証明. x に関する帰納法で証明する．$x = 0 = \alpha_b(0)$ のとき，$y^2 = 1$ より $y = 1 = \alpha_b(1)$ となるのでよい．$x > 0$ とする．仮に $x = y$ とすると $1 = x^2 - bxy + y^2 = x^2 - bx^2 + x^2 = (2-b)x^2$ となるが，これは $b \geq 2$ に矛盾する．よって $x < y$ としてよい．仮定を変形すると

$$y = bx + \frac{1 - x^2}{y}$$

となるが，今 $x > 0$ だから $(1 - x^2)/y \leq 0$ なので

$$y \leq bx \tag{15}$$

を得る．一方, $x < y$ より $x^2 < xy+1$ だから移項して $1-x^2 > -xy$ を得, 両辺を y で割ると $(1-x^2)/y > -x$ なので

$$y = bx + \frac{1 - x^2}{y} > bx - x \tag{16}$$

となる．x_1, y_1 を

$$\begin{cases} x_1 := bx - y, \\ y_1 := x \end{cases}$$

と定義する．式 (15) から $x_1 \geq 0$ である．このとき

$$\begin{aligned} x_1^2 - bx_1y_1 + y_1^2 &= (bx - y)^2 - b(bx - y)x + x^2 \\ &= b^2x^2 - 2bxy + y^2 - b^2x^2 + bxy + x^2 \\ &= x^2 - bxy + y^2 \\ &= 1 \end{aligned}$$

となり，さらに式 (16) より $x > bx - y = x_1$ となる．よって x_1 に対して帰納法の仮定を適用すれば，ある m について $x_1 = \alpha_b(m), y_1 = \alpha_b(m+1)$ となり，x_1, y_1 の定め方から $x = y_1 = \alpha_b(m+1), y = by_1 - x_1 = b\alpha_b(m+1) - \alpha_b(m) = \alpha_b(m+2)$ を得る． □

補題 4.6 を使うと，次の「数列 $\alpha_b(n)$ のどこかに現れる」という関係 (すなわち，$a = \alpha_b(c)$ のグラフの a, b 軸への射影) が Diophantus 的であることを示すことができる．

補題 4.7. 集合

$$\{\, (a, b) \in \mathbb{N}^2 \mid b \geq 2 \wedge \exists n[a = \alpha_b(n)] \,\}$$

は Diophantus 的である．

証明. 補題 4.6 より，$b \geq 2$ に対して

$$\exists n[a = \alpha_b(n)] \iff \exists y[a^2 + bay + y^2 = 1]$$

となるので $b \geq 2 \wedge \exists n[a = \alpha_b(n)]$ は Diophantus 的関係である． □

$\alpha_b(c)$ が Diophantus 的関数であることの証明の前に，必要になる補題をいくつか用意しておく．

補題 4.8. $v > 0, b_1, b_2$ が $b_1 \equiv b_2 \pmod{v}$ を満たすとき，全ての n に対し

$$\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \pmod{v}$$

が成り立つ．

証明. $\alpha_b(n)$ は漸化式で定義されていたので，n に関する帰納法よりわかる． □

系 4.9. $u > 0, w, n$ について $u \mid (w-2)$ ならば

$$\alpha_w(n) \equiv n \pmod{u}$$

が成り立つ．

証明. $w \equiv 2 \pmod{u}$ だから，補題 4.3 と合わせて $\alpha_w(n) \equiv \alpha_2(n) = n \pmod{u}$ を得る． □

補題 4.10. 任意の k, m について

$$\alpha_b(k)^2 \mid \alpha_b(m) \implies \alpha_b(k) \mid m.$$

証明. $\alpha_b(k)^2 \mid \alpha_b(m)$ であると仮定する．m を k で割った商と余りをそれぞれ l, n とおく:

$$m = n + kl \quad (0 \leq n < k). \tag{17}$$

このとき $A_b^m = A_b^n (A_b^k)^l$ だから，補題 4.4 より $\alpha_b(k)$ を法とすれば

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l \pmod{\alpha_b(k)}$$

となるので，$(2,1)$ 成分 (左下成分) を取り出せば

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b(k+1)^l \pmod{\alpha_b(k)}$$

を得る．仮定 $\alpha_b(k)^2 \mid \alpha_b(m)$ より特に $\alpha_b(k) \mid \alpha_b(m)$，つまり $0 \equiv \alpha_b(m) \equiv \alpha_b(n)\alpha_b(k+1)^l \pmod{\alpha_b(k)}$ だから $\alpha_b(k) \mid \alpha_b(n)\alpha_b(k+1)^l$ となる．一方，補題 4.5 より $\alpha_b(k)$ と $\alpha_b(k+1)$ は互いに素だから特に $\alpha_b(k) \nmid \alpha_b(k+1)$ なので $\alpha_b(k) \mid \alpha_b(n)$ でなければならない．さらに，式 (17) より $n < k$ なので補題 4.2 から $\alpha_b(n) < \alpha_b(k)$ でなければならないが，これは $n = 0$ の場合しかありえない．したがって $m = kl$ である．よって，単位行列を E と書くことにすれば

$$
\begin{aligned}
A_b^m &= (A_b^k)^l \\
&= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l && \text{(補題 4.4 より)} \\
&= \left(\begin{pmatrix} b\alpha_b(k) & -\alpha_b(k) \\ \alpha_b(k) & 0 \end{pmatrix} - \begin{pmatrix} \alpha_b(k-1) & 0 \\ 0 & \alpha_b(k-1) \end{pmatrix} \right)^l \\
&= (\alpha_b(k)A_b - \alpha_b(k-1)E)^l \\
&= \sum_{i=0}^{l} (-1)^{l-i} \binom{l}{i} \alpha_b(k)^i \alpha_b(k-1)^{l-i} A_b^i && (A_b \text{ と } E \text{ は可換だから二項定理より})
\end{aligned}
$$

となるから，$\alpha_b(k)^2$ を法とすれば最初の 2 項以外は全て消えて

$$
\begin{aligned}
\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} &= A_b^m \quad \text{(補題 4.4 より)} \\
&\equiv (-1)^l \alpha_b(k-1)^l E + (-1)^{l-1} l \alpha_b(k) \alpha_b(k-1)^{l-1} A_b \pmod{\alpha_b(k)^2}
\end{aligned}
$$

となるので，$(2,1)$ 成分を取り出せば

$$
\alpha_b(m) \equiv (-1)^{l-1} l \alpha_b(k) \alpha_b(k-1)^{l-1} \pmod{\alpha_b(k)^2} \tag{18}
$$

となる．よって仮定 $\alpha_b(k)^2 \mid \alpha_b(m)$ より $\alpha_b(k)^2 \mid l\alpha_b(k)\alpha_b(k-1)^{l-1}$ だから $\alpha_b(k) \mid l\alpha_b(k-1)^{l-1}$ である．一方，補題 4.5 より $\alpha_b(k)$ と $\alpha_b(k-1)$ は互いに素だから特に $\alpha_b(k) \nmid \alpha_b(k-1)$ なので $\alpha_b(k) \mid l$ でなければならない．今 $m = kl$ なので特に $l \mid m$ であるから，所望の結論 $\alpha_b(k) \mid m$ が得られる． □

ようやく準備が整ったので，いよいよ $\alpha_b(c)$ が Diophantus 的関数であることを示そう．

定理 4.11. $b \geq 4$ に対し，2 変数関数 $\alpha_b(c)$ は Diophantus 的関数である．つまり，集合

$$
\{\, (a,b,c) \in \mathbb{N}^3 \mid b \geq 4 \wedge a = \alpha_b(c) \,\} \tag{19}
$$

は Diophantus 的である．

証明のアイデア. 厳密な証明に入る前に，ざっくりと証明の方針について述べよう．証明したいことは，$a = \alpha_b(c)$ のグラフが Diophantus 的集合であることである．言い換えると，パラメーター (a,b,c) が与えられたとき，$a = \alpha_b(c)$ が成り立っているかどうかを Diophantus 的関係を用いて検査したい．我々は $\alpha_b(c)$ を Diophantus 方程式によって計算する術を持たないので (まさに今その方法を探しているところである！)，$\alpha_b(c)$ の値を計算して a と比べる，という方針を採用することはできない．ここで発想を逆転させて考えよう: c から $\alpha_b(c)$ を計算することができないのなら，$a = \alpha_b(j)$ の値から j を逆算すればよいのである．[*11] しかし，いったいどうやって $\alpha_b(j)$ から外側の $\alpha_b(\ )$ を “剥がせば” よいのだろうか？ その鍵は系 4.9 である．どういうことかというと，$u \mid (b-2)$ なる u をとれば $\alpha_b(j) \equiv j \pmod{u}$ となるわけだが，この式は $\alpha_b(j)$ から j を復元しているように見えるということである．では，$a \equiv c \pmod{u}$ であれば $j = c$ が結論できるのかと言えば，答えはもちろん否である．実際，合同であるというだけでは u の倍数の “ずれ” がある可能性を排除することができない．しかし，$b > 2$ のときは $\alpha_b(c) \neq c$ だから，この合同 $\equiv$ を等号 $=$ に安易に変更すること

[*11] そもそも a がある j について $a = \alpha_b(j)$ という形になっているかどうか，ということは補題 4.6 を使えば容易にチェックできる．しかしこの条件は不要であることが後でわかる．

はできない．この問題を解決するために，$a = \alpha_b(j)$ と c の間を “中継” するような別の数を用意する．そのために補題 4.8 を使う．$u \mid (w-2), v \mid (w-b)$ を満たすような u, v, w があるとしよう．このとき

$$\begin{aligned}\alpha_b(j) &\equiv \alpha_w(j) \pmod{v},\\ \alpha_w(j) &\equiv j \pmod{u}\end{aligned}$$

が成り立つ．先程と異なり，w は自由に選べるのでいくらでも大きくとることができ，したがって u, v もいくらでも大きくとることができる．よって u, v を $2a < v, 2c < v$ を満たす程度に大きくとれば，

$$\begin{aligned}a &= \operatorname{arem}(a, v) = \operatorname{arem}(\alpha_b(j), v) = \operatorname{arem}(\alpha_w(j), v),\\ c &= \operatorname{arem}(c, u) = \operatorname{arem}(\alpha_w(j), u)\end{aligned}$$

が成り立つ．つまり，「最小の代表元をとる」と約束しておくことで合同類の代表元の選び方の不定性を除去できる．とはいえ “中継” を担う数 $\alpha_w(n)$ の n をこちらで選ぶことはできないので (その方法を探していたのだった)，どのような n が選ばれても大丈夫なように，次の条件が成り立ってほしい:

$$\text{ある } n \text{ について } \begin{cases} a \equiv \alpha_w(n) \pmod{v}, \\ \alpha_w(n) \equiv c \pmod{u} \end{cases} \text{ が成り立つならば，} j = c \text{ である．} \tag{20}$$

ここで，数列 $(\alpha_w(n) \bmod v)_{n=0}^{\infty}$ は漸化式で定義されているので必ず周期的になるということを指摘しておく．実際，$\alpha_w(n) \bmod v$ は直前の 2 項 $\alpha_w(n-1), \alpha_w(n-2)$ の合同類だけから決まるが，その可能性は v^2 通りしかないので，v^2 以下の周期を持たなければならない．$(\alpha_w(n) \bmod u)_{n=0}^{\infty}$ についても同様である．よって，条件 (20) が成り立つためには次の条件が成り立てば十分である:

$$\alpha_w(j) \equiv \alpha_w(n) \pmod{v} \implies \alpha_w(j) \equiv \alpha_w(n) \pmod{u}. \tag{21}$$

実際，条件 (20) の仮定 $a \equiv \alpha_w(n) \pmod{v}, \alpha_w(n) \equiv c \pmod{u}$ が成り立つとすると，補題 4.8 より $\alpha_w(j) \equiv \alpha_b(j) = a \equiv \alpha_w(n) \pmod{v}$ だから，条件 (21) より $j = \operatorname{arem}(\alpha_w(j), u) = \operatorname{arem}(\alpha_w(n), u) = c$ となり，条件 (20) の結論 $j = c$ が成り立つ．条件 (21) を成り立たせるためには，2 つの数列 $(\alpha_w(n) \bmod u)_{n=0}^{\infty}$ と $(\alpha_w(n) \bmod v)_{n=0}^{\infty}$ それぞれの周期をうまく制御して “同期” をとる必要がある．加えて，単に周期を同期させるだけではなく，数列 $(\alpha_w(n) \bmod v)_{n=0}^{\infty}$ の一周期ぶんの値の中に意図しない “だぶり” がないことも重要である．特別な v に対しては数列 $(\alpha_w(n) \bmod v)_{n=0}^{\infty} = (\alpha_b(n) \bmod v)_{n=0}^{\infty}$ の周期と，その一周期ぶんの値を具体的に決定することができる．多少天下り的ではあるが，$v = \alpha_b(m+1) - \alpha_b(m-1)$ とおこう．$\alpha_b(\ )$ が Diophantus 的関数かもわからないのにどうやって v を定めるのかと思うかもしれないが，実際には補題 4.6 を用いて $\alpha_b(m-1), \alpha_b(m)$ の組を作れば

$$v = b\alpha_b(m) - 2\alpha_b(m-1) = (b\alpha_b(m) - \alpha_b(m-1)) - \alpha_b(m-1) = \alpha_b(m+1) - \alpha_b(m-1)$$

のようにして実現できる．漸化式 $\alpha_b(m+2) = b\alpha_b(m+1) - \alpha_b(m)$ を変形すると $b\alpha_b(m+1) - \alpha_b(m+2) = \alpha_b(m)$ となるので，帰納的に

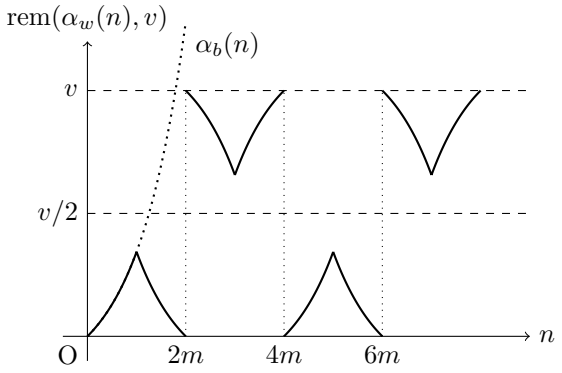
$$
\begin{aligned}
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v},\\
\alpha_b(m+2) &= b\alpha_b(m+1) - \alpha_b(m)\\
&\equiv b\alpha_b(m-1) - \alpha_b(m) \pmod{v}\\
&= \alpha_b(m-2),\\
\alpha_b(m+3) &= b\alpha_b(m+2) - \alpha_b(m+1)\\
&\equiv b\alpha_b(m-2) - \alpha_b(m-1) \pmod{v}\\
&= \alpha_b(m-3),\\
&\dots,\\
\alpha_b(2m-1) &\equiv \alpha_b(1) \pmod{v},\\
\alpha_b(2m) &\equiv \alpha_b(0) \pmod{v}
\end{aligned}
$$

がわかる．さらに，漸化式によって数列 $\alpha_b(n)$ を $n < 0$ の場合に拡張すると，帰納法により $\alpha_b(-n) = b\alpha_b(-n+1) - \alpha_b(-n+2) = -(b\alpha_b(n-1) - \alpha_b(n-2)) = -\alpha_b(n)$ がわかる．よって帰納的に

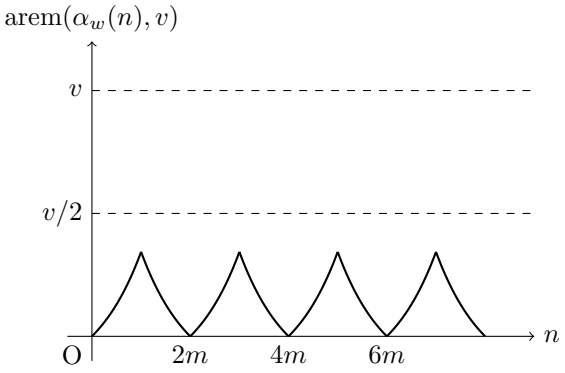
$$
\begin{aligned}
\alpha_b(2m+1) &\equiv b\alpha_b(2m) - \alpha_b(2m-1) \pmod{v}\\
&\equiv b\alpha_b(0) - \alpha_b(1) \pmod{v}\\
&= \alpha_b(-1) = -\alpha_b(1),\\
\alpha_b(2m+2) &\equiv b\alpha_b(2m+1) - \alpha_b(2m) \pmod{v}\\
&\equiv b\alpha_b(-1) - \alpha_b(0) \pmod{v}\\
&= \alpha_b(-2) = -\alpha_b(2),\\
&\dots,\\
\alpha_b(4m-1) &\equiv -\alpha_b(2m-1) \equiv -\alpha_b(1) \pmod{v},\\
\alpha_b(4m) &\equiv -\alpha_b(2m) \equiv -\alpha_b(0) \pmod{v}
\end{aligned}
$$

がわかる．これ以降は $\alpha_b(4m+1) = b\alpha_b(4m) - \alpha_b(4m-1) \equiv -(b\alpha_b(2m) - \alpha_b(2m-1)) = -\alpha_b(2m+1) \equiv \alpha_b(1) \pmod{v}$ となって最初に戻るので，数列 $(\alpha_b(n) \bmod v)_{n=0}^{\infty} = (\mathrm{rem}(\alpha_w(n), v))_{n=0}^{\infty}$ は周期 $4m$ を持つ．しかも，$b \geq 4$ であるとすれば $v = b\alpha_b(m) - 2\alpha_b(m-1) \geq 4\alpha_b(m) - 2\alpha_b(m) = 2\alpha_b(m)$ だから，$0 \leq n \leq m$ で狭義単調増加となり値の重複は起こらない (図 3a)．さらに，rem を arem に変更すると負号が消えるので，$\mathrm{arem}(\alpha_w(n), v)$ の周期は $2m$ となり，しかも m ずつに分けると対称的になっている (図 3b)．ここでさらに $u \mid m$ という条件を課せば，$\mathrm{arem}(\alpha_w(n), u)$ の周期が $\mathrm{arem}(\alpha_w(n), v)$ の周期を割ることになる (図 3c)．しかし，$u \mid m$ という制約を設けるためには，一見すると v を定義するのに使った $\alpha_b(m)$ から m を取り出す必要があるように思われる．実は，この条件を課すために役に立つのが補題 4.10 である．つまり，補題 4.6 を使って $u = \alpha_b(k)$ の形にして，$u^2 \mid \alpha_b(m)$ というより強い条件で置き換えればよいのである．以上の設定の下で条件 (21) が成り立つのはほとんど明らかであろう． □

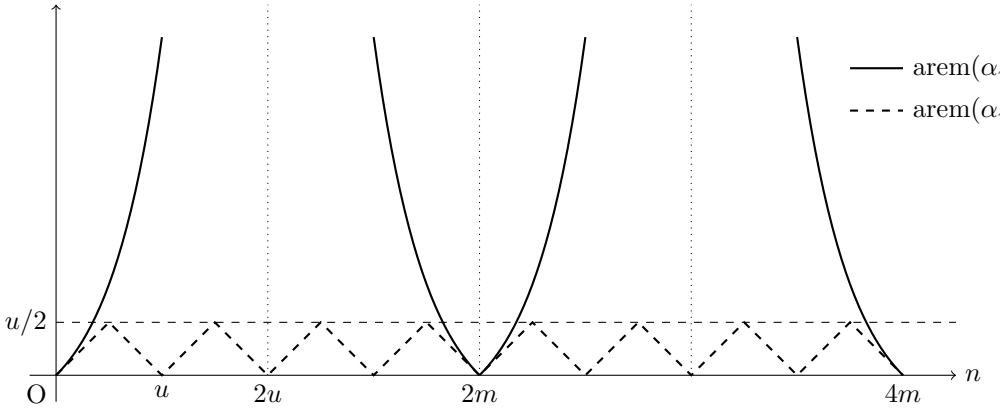
それでは，上で述べた証明の大まかなアイデアを厳密な証明に書き直そう．



(a) $v = \alpha_b(m+1) - \alpha_b(m-1)$ とした場合



(b) rem を arem に変更する



(c) $u \mid m$ という条件を付けた場合 (ここでは $m = 2u$)

図 3: Diophantus 的関係による数列の周期の制御

証明. 以下の連立 Diophantus 方程式[*12]が集合 (19) を定義することを示す.

$$\begin{cases} b \geq 4, & (22.1)\\ u^2 - buu_1 + u_1^2 = 1, & (22.2)\\ r < s, & (22.3)\\ r^2 - brs + s^2 = 1, & (22.4)\\ u^2 \mid s, & (22.5)\\ v = bs - 2r, & (22.6)\\ w > 2, & (22.7)\\ x^2 - wxx_1 + x_1^2 = 1, & (22.8)\\ v \mid (w - b), & (22.9)\\ u \mid (w - 2), & (22.10)\\ a = \mathrm{arem}(x, v), & (22.11)\\ 2a < u, & (22.12)\\ c = \mathrm{arem}(x, u). & (22.13) \end{cases}$$

[*12] 正確には方程式ではないが，全ての条件が Diophantus 的関係なので Diophantus 方程式に書き直すことができる.

まず，連立 Diophantus 方程式 (22.1)–(22.13) が解を持つならば $b \geq 4 \wedge a = \alpha_b(c)$ であることを示す．(22.1) より $b \geq 4$ だから，あとは $a = \alpha_b(c)$ であることを示せばよい．(22.1)，(22.2) と補題 4.6 よりある自然数 k が存在して

$$u = \alpha_b(k) \tag{23}$$

が成り立つ．(22.1)，(22.3)，(22.4) と補題 4.6 よりある自然数 $m > 0$ が存在して

$$r = \alpha_b(m-1), \tag{24.1}$$
$$s = \alpha_b(m) \tag{24.2}$$

が成り立つ．(23)，(24.2)，(22.5) と補題 4.10 より

$$u \mid m \tag{25}$$

が成り立つ．(22.6) に (24.1)，(24.2) を代入すれば

$$\begin{aligned} v &= b\alpha_b(m) - 2\alpha_b(m-1) && (26.1)\\ &= (b\alpha(m) - \alpha_b(m-1)) - \alpha_b(m-1) \\ &= \alpha_b(m+1) - \alpha_b(m-1) && (26.2) \end{aligned}$$

となる．(22.7)，(22.8) と補題 4.6 よりある自然数 n が存在して

$$x = \alpha_w(n) \tag{27}$$

が成り立つ．(22.9) より $w \equiv b \pmod{v}$ だから (27) と補題 4.8 より

$$x = \alpha_w(n) \equiv \alpha_b(n) \pmod{v} \tag{28}$$

が成り立つ．(22.10) より $w \equiv 2 \pmod{u}$ だから (27) と系 4.9 より

$$x = \alpha_w(n) \equiv n \pmod{u} \tag{29}$$

が成り立つ．n を $2m$ で割れば

$$n = 2lm \pm j, \tag{30.1}$$
$$j \leq m \tag{30.2}$$

を満たす l, j (と符号 $\pm$) が一意に定まることがわかる．補題 4.4 と (26.2) より

$$A_b^m = \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} = -(A_b^m)^{-1} \pmod{v}$$

となるから，両辺に A_b^m を掛ければ

$$(A_b^m)^2 \equiv -(A_b^m)^{-1} A_b^m = -E \pmod{v} \tag{31}$$

が成り立つ．(30.1)，(31) より

$$\begin{aligned} A_b^n &= A_b^{2lm\pm j} && ((30.1)\text{ より}) \\ &= ((A_b^m)^2)^l (A_b^j)^{\pm 1} \\ &\equiv (-E)^l (A_b^j)^{\pm 1} \pmod v && ((31)\text{ より}) \\ &= \pm (A_b^j)^{\pm 1} && (\text{複号同順でない}) \end{aligned}$$

が成り立つから，$(2,1)$ 成分を取り出せば

$$\alpha_b(n) \equiv \pm \alpha_b(j) \pmod v \tag{32}$$

を得る．(30.2)，補題 4.2，(22.1)，(26.1) より

$$\begin{aligned} 2\alpha_b(j) &\le 2\alpha_b(m) && ((30.2)\text{ と補題 4.2 より}) \\ &\le (b-2)\alpha_b(m) && ((22.1)\text{ より}) \\ &= b\alpha_b(m) - 2\alpha_b(m) \\ &< b\alpha_b(m) - 2\alpha_b(m-1) && (\text{補題 4.2 より}) \\ &= v && ((26.1)\text{ より}) \end{aligned} \tag{33}$$

が成り立つ．(22.11)，(28)，(32)，(33) より

$$\begin{aligned} a &= \mathrm{arem}(x, v) && ((22.11)\text{ より}) \\ &= \mathrm{arem}(\alpha_b(n), v) && ((28)\text{ より}) \\ &= \alpha_b(j) && ((32),\ (33)\text{ より}) \end{aligned} \tag{34}$$

が成り立つ．補題 4.2，(34)，(22.12) より

$$\begin{aligned} 2j &\le 2\alpha_b(j) && (\text{補題 4.2 より}) \\ &= 2a && ((34)\text{ より}) \\ &< u && ((22.12)\text{ より}) \end{aligned} \tag{35}$$

が成り立つ．(22.13)，(29)，(25)，(30.1)，(35) より

$$\begin{aligned} c &= \mathrm{arem}(x, u) && ((22.13)\text{ より}) \\ &= \mathrm{arem}(n, u) && ((29)\text{ より}) \\ &= j && ((25),\ (30.1),\ (35)\text{ より}) \end{aligned} \tag{36}$$

が成り立つ．よって (34)，(36) より

$$a = \alpha_b(j) = \alpha_b(c)$$

が成り立つ．

次に，逆向きを示す．すなわち，a, b, c が $b \ge 4 \wedge a = \alpha_b(c)$ を満たすならば，連立 Diophantus 方程式 (22.1)–(22.13) を満たす解 $u, u_1, r, s, v, w, x, x_1$ が存在することを示す．(22.1) が成り立っていることは明らか．補題 4.2 より $2a < \alpha_b(k)$ となるような $k > 0$ がとれる．さらに，補題 4.5 より数列 $\alpha_b(n)$ の隣り合う 2 項が両方とも偶数であることはないから，$\alpha_b(k)$ は奇数であるとしてよい．よって (23) のように $u := \alpha_b(k)$ とおけば (22.12) が成り立つ．$u_1 := \alpha_b(k+1)$ とおけば式 (14) より (22.2) が成り立つ．

$m := ku, r := \alpha_b(m-1), s := \alpha_b(m)$ とおけば補題 4.2 より (22.3) が，式 (14) より (22.4) が成り立つ．式 (18) を用いると

$$\begin{aligned} s = \alpha_b(m) = \alpha_b(ku) &\equiv (-1)^{u-1} u \alpha_b(k) \alpha_b(k-1)^{u-1} \pmod{u^2} \\ &= (-1)^{u-1} u^2 \alpha_b(k-1)^{u-1} \\ &\equiv 0 \pmod{u^2} \end{aligned}$$

となるので (22.5) が成り立つ．次に，$v := bs - 2r$ とおくと，補題 4.2 より

$$\begin{aligned} v = bs - 2r &= b\alpha_b(m) - 2\alpha_b(m-1) \\ &\geq 4\alpha_b(m) - 2\alpha(m-1) && (b \geq 4 \text{ より}) \\ &= 2\alpha_b(m) + 2(\alpha_b(m) - \alpha_b(m-1)) \\ &> 2\alpha_b(m) && (\text{補題 4.2 より}) \\ &\geq 0 \end{aligned} \tag{37}$$

となるので $v \in \mathbb{N}$ となり (22.6) が成り立つ．u と v が互いに素であることを示す．$d \mid u, d \mid v$ と仮定すると，今 $u^2 \mid s$ だから $d \mid s$ でもある．よって $d \mid (bs - v) = 2r$ となる．今 u は奇数だったから d も奇数であり，よって $d \mid r$ を得る．補題 4.5 より $r = \alpha_b(m-1)$ と $s = \alpha_b(m)$ は互いに素だから $d = 1$ でなければならない．よって u と v は互いに素だから，**中国剰余定理** (Chinese remainder theorem) より環の同型

$$\begin{array}{ccc} \mathbb{Z}/uv\mathbb{Z} & \cong & \mathbb{Z}/u\mathbb{Z} \times \mathbb{Z}/v\mathbb{Z} \\ N \bmod uv & \mapsto & (N \bmod u, N \bmod v) \end{array}$$

がある．したがって $(2 \bmod u, b \bmod v) \in \mathbb{Z}/u\mathbb{Z} \times \mathbb{Z}/v\mathbb{Z}$ に対応する $w \bmod uv \in \mathbb{Z}/uv\mathbb{Z}$ がとれる．必要なら w を $w + 3uv$ で置き換えることで (22.7) が成り立つとしてよい．このとき w のとり方から (22.9)，(22.10) が成り立つ．$x := \alpha_w(c), x_1 := \alpha_w(c+1)$ とおくと式 (14) より (22.8) が成り立つ．今 $w \equiv b \pmod{v}$ だから補題 4.8 より

$$x = \alpha_w(c) \equiv \alpha_b(c) = a \pmod{v}$$

であり，さらに式 (37) より

$$v = bs - 2r > 2\alpha_b(m) = 2a$$

であるので (22.11) が成り立つ．最後に，今 $u \mid (w-2)$ だから系 4.9 より

$$x = \alpha_w(c) \equiv c \pmod{u}$$

であり，さらに補題 4.2 と $2a < u$ より

$$2c \leq 2\alpha_b(c) = 2a < u$$

であるので (22.13) が成り立つ． □

4.2 指数関数 $a = b^c$ が Diophantus 的であることの証明

ここまでの長い準備によって，$\alpha_b(c)$ が Diophantus 的関数であることがわかった．ここまで来てしまえば，2 項関数 b^c が Diophantus 的であることを示すのはそれほど難しくない．[*13]証明にあたり重要なことは，b が大きいとき，$\alpha_b(n)$ は漸近的には指数関数的 b^n とほぼ同じ速さで増大するということである．

補題 4.12. 任意の $b \geq 2, n$ について

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n$$

となる．

証明. n に関する帰納法で証明する．$n = 0$ のときは $(b-1)^0, \alpha_b(0+1), b^0$ は全て 1 なのでよい．$n = 1$ のときは $(b-1)^1, \alpha_b(1+1), b^1$ はそれぞれ $b-1, b, b$ なのでよい．n 以下で成り立つとすると，帰納法の仮定から

$$\alpha_b((n+1)+1) = b\alpha_b(n+1) - \alpha_b(n) \begin{cases} \leq b \cdot b^n - (b-1)^{n-1} \leq b^{n+1}, \\ \geq b\alpha_b(n+1) - \alpha_b(n+1) = (b-1)\alpha_b(n+1) \geq (b-1)^{n+1} \end{cases}$$

となる． □

一方で，求めたいのは固定された b, c に対する b^c である．実は，任意の $b, c \geq 0$ に対し，

$$\lim_{x \to \infty} \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = b^c \tag{38}$$

が成り立つことを示すことができる．Diophantus 方程式はもちろん lim を計算する能力を持たないが，極限が b^c に収束するということは，十分に大きな x に対しては

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < b^c + 1$$

が成り立つということである．また，$x \geq 2$ なら補題 4.12 より

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} \geq \frac{(bx+3)^c}{x^c} = \left(b + \frac{3}{x}\right)^c \geq b^c$$

となるので，式 (38) の極限は b^c に「上から」近づく．したがって x が十分に大きければ，比の整数部分をとることで，b^c の正確な値を

$$\alpha_{bx+4}(c+1) \operatorname{div} \alpha_x(c+1) = b^c$$

と計算できることになる．具体的に x がどのくらい大きければ十分なのか，という保証を与えるのが次の補題である．

補題 4.13. $x > 16(cb^c + 1)$ ならば

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < b^c + 1$$

が成り立つ．さらに，式 (38) が成り立つ．

[*13] ただし，$0^0 := 1$ と約束しておく．

証明. b, c の値で場合分けして証明する.

- $b = c = 0$ のとき:
$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = \frac{\alpha_4(1)}{\alpha_x(1)} = 1.$$
- $b = 0, c > 0$ のとき:
$x > 16$ だから,
$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = \frac{\alpha_4(c+1)}{\alpha_x(c+1)} \leq \frac{4^c}{(x-1)^c} \leq \left(\frac{4}{16}\right)^c < 1 = 0^c + 1.$$
また，明らかに $\lim_{x\to\infty} 4^c/(x-1)^c = 0 = 0^c$ である.
- $b > 0$ のとき:
$\mathbb{R}$ 上の関数 $F(X)$ を $F(X) := (1-X)^{2c}$ で定めると，$F(0) = 1$ であり，$X = 0$ における微分係数は $F'(0) = 2c$ である．よって $X = 0$ における接線は $1 - 2cX$ で表されるので，$F(X)$ が偶数次であることから下に凸であることと合わせて
$$1 - 2cX \leq (1-X)^{2c} \tag{39}$$
を得る (図 4).

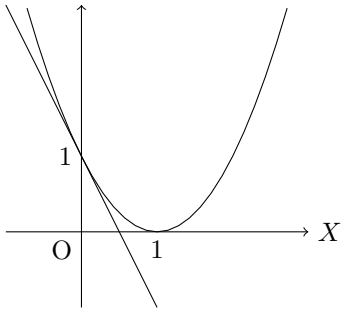


図 4: 関数 $F(X) = (1-X)^{2c}$ と $1 - 2cX$ のグラフ

よって,
$$\begin{aligned}\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} &\leq \frac{(bx+4)^c}{(x-1)^c} = \frac{(x+4/b)^c}{(x-1)^c}b^c = \frac{(1+4/bx)^c}{(1-1/x)^c}b^c \\ &\leq \frac{(1+4/x)^c}{(1-1/x)^c}b^c = \frac{(1+4/x)^c(1-4/x)^c}{(1-1/x)^c(1-4/x)^c}b^c = \frac{(1-16/x^2)^c}{(1-1/x)^c(1-4/x)^c}b^c\end{aligned}$$
今 $x > 16$ だから分母は正であり，また $1 - 16/x^2 < 1$ だから
$$\begin{aligned}&< \frac{b^c}{(1-1/x)^c(1-4/x)^c} \\ &< \frac{b^c}{(1-4/x)^c(1-4/x)^c} = \frac{b^c}{(1-4/x)^{2c}}\end{aligned}$$
式 (39) で $X = 4/x$ とすれば
$$\leq \frac{b^c}{1-8c/x} = \frac{b^c(1+16c/x)}{(1-8c/x)(1+16c/x)} = \frac{b^c(1+16c/x)}{1+(8c/x)(1-16c/x)}$$

$x > 16c$ より $1 - 16c/x > 0$ ゆえ $1 + (8c/x)(1 - 16c/x) \geq 1$ なので

$$\leq b^c \left(1 + \frac{16c}{x}\right)$$

今 $x > 16cb^c$ だから $16c/x < 1/b^c$ なので

$$< b^c \left(1 + \frac{1}{b^c}\right) = b^c + 1.$$

また，明らかに $\lim_{x\to\infty} b^c(1 + 16c/x) = b^c$ である． □

さて，それでは b^c が Diophantus 的関数であることを示して本節を終えよう．

定理 4.14 (Matiyasevich, 1970). 2 変数の指数関数 b^c は Diophantus 的関数である．

証明. $x := 16(c\alpha_{b+1}(c+1)+1)+1$ とおけば，補題 4.12 より $x > 16(cb^c+1)$ となり，x は補題 4.13 の条件を満たす．よって，関係 $a = b^c$ は連立 Diophantus 方程式

$$\begin{cases} x = 16c\alpha_{b+1}(c+1) + 17, \\ a = \alpha_{bx+4}(c+1) \operatorname{div} \alpha_x(c+1) \end{cases}$$

によって定義される． □

注意 4.15. 本稿では 2 階線形回帰数列 $\alpha_b(n)$ が Diophantus 的であることを利用して指数関数 b^c が Diophantus 的であることを示したが，もちろんこれは唯一の方法というわけではない．実際，1952 年には Robinson によって指数関数が Diophantus 的であるための十分条件がいくつか示されており，指数関数的に増大するような Diophantus 的関数が存在すれば指数関数 b^c も Diophantus 的であることが示されている．[*14]Matiyasevich による 1970 年のオリジナルの証明では，補題 4.6 の方程式 $x^2 - bxy + y^2 = 1$ の代わりに Pell 方程式 $x^2 - (a^2-1)y^2 = 1$ を用いることで，$\phi_{n+2} = \phi_{n+1} + \phi_n$ で定義される Fibonacci 数列 ϕ_n について $v = \phi_{2u}$ が Diophantus 的関数であることを示している．この方針での証明が書かれた文献としては例えば廣瀬 [9, 7 章] や Davis [10] がある．

また，$\alpha_b(n)$ を用いる代わりに，よく似た 2 階線形回帰数列 $\gamma_b(n+2) = b\gamma_b(n+1) + \gamma_b(n)$ $(b \geq 1)$ を用いることもできる [1, Exercise 2.5]．$\gamma_b(n)$ で特に $b = 1$ とすれば $\gamma_1(n) = \phi_n$ となる．

いずれにせよ，重要なのは $\alpha_b(n)$ や ϕ_n など個々の数列の性質ではなく，指数関数的に増大する数列たちの中に Diophantus 的なものが存在するということである．

まとめ

- 線形回帰数列 $\alpha_b(n)$ の値として現れる自然数は，コンパニオン行列 A_b の行列式から定まる，$\alpha_b(n)$ と $\alpha_b(n+1)$ の間の関係式によって完全に特徴付けられる．
- 特別な v を法とすることで $(\alpha_b(n) \bmod v)_{n=0}^{\infty}$ の周期をうまく制御すると，$\alpha_b(c)$ が b, c に関する Diophantus 的関数であることがわかる．
- 十分大きな x について $b^c \leq \alpha_{bx+4}(c+1)/\alpha_x(c+1) < b^c+1$ であることを利用すると，b^c が Diophantus 的関数であることがわかる．

[*14] 例えば，Diophantus 的関数 $F(u)$ が $\forall u[F(u) < u^u], \forall n \exists u[F(u) \geq u^n]$ を満たせば $a = b^c$ も Diophantus 的，などである．

5　有限列のコード化

3 節の最初で，Turing 機械 M に対応する Diophantus 方程式を作りたいと述べた．これは Diophantus 的集合の言葉で言えば，与えられた Turing 機械 M が停止することを表現する Diophantus 的関係を構成したいわけである．これを素直に実装するとすれば，Turing 機械 M に対し「自然数の n 個組 $(a_1, \ldots, a_n)$ が M の計算履歴を表しているかどうかを検査するような Diophantus 的関係 $R(a_1, \ldots, a_n)$」を構成することになるだろう．ところが，ここで次のような問題が生じる: 入力の機械 M によって使用するテープの長さも，停止するまでのステップ数も異なるのに，その計算履歴をあらかじめ固定された個数の変数 $a_1, \ldots, a_n$ でどうやって表せばよいのだろうか？ この問題を解決するために，本節では自然数の任意の長さの有限列を 1 つの自然数に「コード化」する技法を開発する．

5.1　Cantor コード化

まず，ウォームアップとして任意長ではなく固定長の列をコード化する方法を与える．この手法は今後の議論に本質的に必要だというわけではないが，これにより 6 節の議論が少しだけ簡単になる．

よく知られているように，**Cantor の対関数** (Cantor's pairing function)

$$\mathrm{Cantor}(a, b) := \frac{(a+b)(a+b+1)}{2} + a$$

は $\mathbb{N} \times \mathbb{N}$ から $\mathbb{N}$ への全単射である[*15]．よって $c = \mathrm{Cantor}(a, b)$ の値からもとの a, b を復元する関数 $a = \mathrm{ElemA}(c), b = \mathrm{ElemB}(c)$ が存在し，しかも

$$\begin{aligned} a = \mathrm{ElemA}(c) &\iff \exists y[(a+y)(a+y+1) + 2a = 2c], \\ b = \mathrm{ElemB}(c) &\iff \exists x[(x+b)(x+b+1) + 2x = 2c] \end{aligned}$$

のようにして Diophantus 的関数になっていることがわかる．

Cantor の対関数を繰り返し適用することで，任意の n 対して，長さ n のコード化関数 Cantor_n を帰納的に作ることができる:

$$\begin{aligned} \mathrm{Cantor}_1(a_1) &:= a_1, \\ \mathrm{Cantor}_{n+1}(a_1, \ldots, a_{n+1}) &:= \mathrm{Cantor}_n(a_1, \ldots, a_{n-1}, \mathrm{Cantor}(a_n, a_{n+1})). \end{aligned}$$

また，$c = \mathrm{Cantor}_n(a_1, \ldots, a_n)$ の値から m 番目の成分 a_m を復元する関数 $\mathrm{Elem}_{n,m}(c)$ は

$$a = \mathrm{Elem}_{n,m}(c) \iff \exists x_1 \cdots \exists x_{m-1} \exists x_{m+1} \cdots \exists x_n [2^{2^n} \mathrm{Cantor}_n(x_1, \ldots, x_{m-1}, a, x_{m+1}, \ldots, x_n) = 2^{2^n} c]$$

のように定義できる．[*16] このとき $\mathrm{Cantor} = \mathrm{Cantor}_2, \mathrm{ElemA} = \mathrm{Elem}_{2,1}, \mathrm{ElemB} = \mathrm{Elem}_{2,2}$ である．

[*15] 証明は例えば拙著 [11] を参照のこと．

[*16] この定義における 2^{2^n} は $\mathrm{Cantor}_n(a_1, \ldots, a_n)$ の係数の分母を払って整数係数にするためのものである．ここで n は関数 $\mathrm{Elem}_{n,m}$ の引数ではないので，2^{2^n} はただの定数であり，指数関数が Diophantus 的関数であることは用いていないことに注意せよ．

5.2 位取りコード化

次に，Cantor コード化より強力な，位取り記数法を利用した任意長の列のコード化の手法を導入する．

定義 5.1 (位取りコード化 (positional coding)). 三つ組 (a,b,n) が列 $(a_1,\dots,a_n)$ の**位取りコード** (positional code) [*17]であるとは，2 条件

1. $b \geq 2$ かつ各 $i = 1,\dots,n$ に対して $a_i < b$,
2. $a = a_n b^{n-1} + a_{n-1} b^{n-2} + \cdots + a_2 b^1 + a_1 b^0$

を満たすときをいう．すなわち，a の b 進展開が n 桁であり，なおかつ下から i 桁目の数字が a_i になっていることをいう．また，このとき a を **cipher**，b を**底** (base)，n を**長さ** (length) と呼ぶ．

特に，$(0,b,0)$ は空列 () のコードである．

補題 5.2. 以下の関係・関数は全て Diophantus 的である．

1. (a,b,c) が何らかの列のコードであることを表す 3 項関係 $\mathrm{Code}(a,b,c)$,
2. コードの cipher が a，底が b であるような列の d 番目の成分を返す関数 $\mathrm{Elem}(a,b,d)$, [*18]
3. (a,b,c) が「コードが (a_1,b,c_1) であるような列」と「コードが (a_2,b,c_2) であるような列」を連結した列のコードであることを表す 7 項関係 $\mathrm{Concat}(b,a,c,a_1,c_1,a_2,c_2)$.

証明. 以下のようにすればよい．

1. $\mathrm{Code}(a,b,c) \iff b \geq 2 \wedge a < b^c$.
2. $a = (a_n b^{n-1} + \cdots + a_{d+1} b^d) + a_d b^{d-1} + (a_{d-1} b^{d-2} + \cdots + a_2 b^1 + a_1 b^0)$ と分割して考えれば

$$e = \mathrm{Elem}(a,b,d) \iff \exists x \exists y \exists z [d = z+1 \wedge a = x b^d + e b^z + y \wedge e < b \wedge y < b^z].$$

3. $\mathrm{Concat}(b,a,c,a_1,c_1,a_2,c_2) \iff \mathrm{Code}(a_1,b,c_1) \wedge \mathrm{Code}(a_2,b,c_2) \wedge a = a_2 b^{c_1} + a_1 \wedge c = c_1 + c_2$. □

底が異なる列の連結については 5.4 節で行う．

5.3 二項係数，階乗，素数

位取りコード化の副産物として，二項係数が Diophantus 的であることがわかる．

補題 5.3. 任意の n,k $(k \leq n)$ に対して $\binom{n}{k} \leq 2^n$ が成り立つ．

証明. $n = 0$ や $k = 0, n$ のときは明らか．その他のときは n に関する帰納法により

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \leq 2^n + 2^n = 2^{n+1}$$

を得る． □

[*17] 本稿では位取りコード以外のコードは用いないので，以降は単にコードと呼ぶ．
[*18] ただし，d が 0 のときは未定義とし，d が列の長さより大きいときは 0 を返す．

命題 5.4. 二項係数 $\binom{n}{m}$ は Diophantus 的関数である．[*19]

証明. 二項定理より

$$(b+1)^n = \sum_{k=0}^{n} \binom{n}{k} b^k$$

だから，補題 5.3 より $b = 2^n + 1$ に対して三つ組 $((b+1)^n, b, n+1)$ は列

$$\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n} \right)$$

のコードになっている．よって，

$$c = \binom{n}{m} \iff c = \mathrm{Elem}((2^n+2)^n, 2^n+1, m+1)$$

である． □

次に，

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

であることを利用すると，実は階乗 $m!$ も Diophantus 的関数であることを示すことができる．実際，計算により

$$\begin{aligned} m! &= \frac{1}{\binom{n}{m}} \frac{n!}{(n-m)!} \\ &= \frac{1}{\binom{n}{m}} n(n-1)(n-2)\cdots(n-(m-1)) \\ &= \frac{n^m}{\binom{n}{m}} 1 \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{m-1}{n}\right) \end{aligned}$$

となるが，最左辺は n によらないので $n \to \infty$ とすれば

$$\lim_{n\to\infty} \frac{n^m}{\binom{n}{m}} = m!$$

を得る．あとは 4.2 節と同様にして，「十分大きな」n に対して

$$m! = n^m \operatorname{div} \binom{n}{m}$$

が成り立つ，という寸法である．以下では，n がどのくらい大きければ十分かを具体的に与える．

補題 5.5. 任意の m に対し

$$\frac{2^{m-1}}{(m+1)^m} < \frac{1}{m!}$$

が成り立つ．

[*19] ただし，$m > n$ のときは $\binom{n}{m} = 0$ とする．

証明. m に関する帰納法で示す．$m = 0, 1$ のときは明らか．その他のときは，帰納法の仮定

$$\frac{(m+1)^m}{m!2^{m-1}} > 1$$

から

$$\begin{aligned}
\frac{(m+2)^{m+1}}{(m+1)!2^m} &= \frac{(m+2)^{m+1}}{2(m+1)^{m+1}} \frac{(m+1)^m}{m!2^{m-1}} \\
&> \frac{1}{2}\left(\frac{m+2}{m+1}\right)^{m+1} \\
&= \frac{1}{2}\left(1 + \frac{1}{m+1}\right)^{m+1} \\
&= \frac{1}{2}\left(1 + (m+1)\frac{1}{m+1} + \cdots\right) \\
&\geq \frac{1}{2} \cdot 2 = 1
\end{aligned}$$

を得る． □

補題 5.6. $n \geq (m+1)^{m+2}$ のとき

$$m! \leq \frac{n^m}{\binom{n}{m}} < m! + 1$$

が成り立つ．

証明. まず，

$$m!\binom{n}{m} = \frac{n!}{(n-m)!} = n(n-1)\cdots(n-m+1) \leq n^m$$

だから $m! \leq n^m / \binom{n}{m}$ であることはよい．もう一方を示す．$m = 0, 1$ のときは明らかだから $m \geq 2$ と仮定してよい．計算により

$$\begin{aligned}
\frac{n^m}{\binom{n}{m}} < m! + 1 &\iff n^m \frac{(n-m)!}{n!} < \frac{1}{m!}(m! + 1) \\
&\iff n^m \frac{1}{n}\frac{1}{n-1}\cdots\frac{1}{n-(m-1)} < \frac{1}{m!}(m! + 1) \\
&\iff \frac{1}{1-\frac{1}{n}}\cdots\frac{1}{1-\frac{m-1}{n}} < 1 + \frac{1}{m!} \qquad (40)
\end{aligned}$$

がわかるので，不等式 (40) を示せばよい．これも計算すれば

$$\begin{aligned}
\frac{1}{1-\frac{1}{n}}\cdots\frac{1}{1-\frac{m-1}{n}} &\leq \left(\frac{1}{1-\frac{m-1}{n}}\right)^{m-1} \\
&\leq \left(\frac{1}{1-\frac{m-1}{(m+1)^{m+2}}}\right)^{m-1} \\
&\leq \left(\frac{1}{1-\frac{1}{(m+1)^{m+1}}}\right)^{m-1} \\
&= \left(\frac{(m+1)^{m+1}}{(m+1)^{m+1}-1}\right)^{m-1}
\end{aligned}$$

一般に，$0 < x < y < z$ ならば $z/y < (z-x)/(y-x)$ だから，$m \geq 1$ と合わせて

$$\begin{aligned}
&< \left(\frac{(m+1)^{m+1} - ((m+1)^{m+1} - (m+1)^m - 1)}{(m+1)^{m+1} + 1 - ((m+1)^{m+1} - (m+1)^m - 1)} \right)^{m-1} \\
&= \left(\frac{(m+1)^m + 1}{(m+1)^m} \right)^{m-1} \\
&= \left(1 + \frac{1}{(m+1)^m} \right)^{m-1}
\end{aligned}$$

$m \geq 2$ だから二項定理より

$$\begin{aligned}
&= 1 + \sum_{k=1}^{m-1} \binom{m-1}{k} \frac{1}{(m+1)^{mk}} \\
&\leq 1 + \frac{1}{(m+1)^m} \sum_{k=1}^{m-1} \binom{m-1}{k}
\end{aligned}$$

$m \geq 2$ と二項定理より $(1+1)^{m-1} = \sum_{k=0}^{m-1} \binom{m-1}{k}$ だから

$$\begin{aligned}
&= 1 + \frac{2^{m-1} - 1}{(m+1)^m} \\
&< 1 + \frac{2^{m-1}}{(m+1)^m}
\end{aligned}$$

補題 5.5 より

$$< 1 + \frac{1}{m!}$$

となる． □

命題 5.7. 階乗 $m!$ は Diophantus 的関数である．

証明. 補題 5.6 より，関係 $a = m!$ は連立 Diophantus 方程式

$$\begin{cases} n \geq (m+1)^{m+2}, \\ a = n^m \operatorname{div} \binom{n}{m} \end{cases}$$

によって定義される． □

階乗が Diophantus 的関数であることがわかると，素数全体の集合が Diophantus 的集合であることが直ちにわかる．

系 5.8. a が素数であることを表す 1 項関係 $\mathrm{Prime}(a)$ は Diophantus 的である．

証明. $\mathrm{Prime}(a) \iff a > 1 \wedge \gcd(a, (a \dot{-} 1)!) = 1$. □

5.4 底の異なるコードの比較

ここでは底 b の異なる 2 つのコードを比較する手法を開発する．具体的には，$(a_1, b_1, c_1), (a_2, b_2, c_2)$ が同じ列のコードであることを表す 6 項関係 $\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2)$ と，底の異なるコードの連結を表す 9 項関係 $\mathrm{Concat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2)$ がともに Diophantus 的であることを証明する．

まず，初等整数論におけるいくつかの定理を用意するところから始める．

定義 5.9 (p 進付値). p を素数，$n \geq 1$ を自然数とする．このとき，n を p で割り切れる回数を p **進付値** (p-adic valuation) と言い，本稿では $\deg_p n$ で表す．[*20]つまり，$d = \deg_p n$ のとき $p^d \mid n, p^{d+1} \nmid n$ である．

補題 5.10 (Legendre の公式 (Legendre's formula)[*21]). 素数 p と自然数 n に対し，

$$\deg_p(n!) = \sum_{i=1}^{\infty} n \operatorname{div} p^i.$$

証明. $n!$ を素因数分解したときに現れる p の個数を数えればよい．p は素数だから，$1, 2, \ldots, n$ のそれぞれに含まれる p の個数を数えて足せばよい．$1, 2, \ldots, n$ の中に，p の倍数はちょうど $n \operatorname{div} p$ 個ある．また，p^2 の倍数はちょうど $n \operatorname{div} p^2$ 個ある．同様にして，p^i の倍数はちょうど $n \operatorname{div} p^i$ 個ある．したがってこれらの総和は $\deg_p(n!)$ に等しい (図 5). □

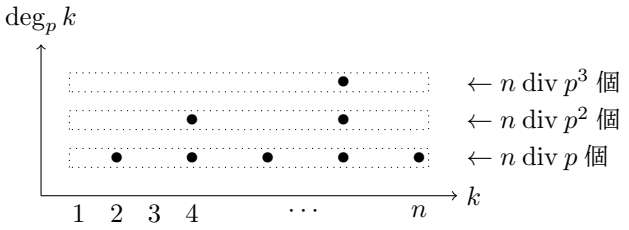


図 5: $p = 2, n = 10$ の場合の Legendre の公式

定理 5.11 (Kummer の定理 (Kummer's theorem) [1, Appendix 3]). p を素数，$m, n \geq 0$ とする．$\deg_p \binom{m+n}{n}$ は m, n をそれぞれ p 進展開して $m + n$ を筆算で計算したときに繰り上がりが発生する回数に等しい．

例 5.12. 例えば $p = 3, m = 14, n = 19$ とすると，$m, n, m + n$ の 3 進展開はそれぞれ $m = (112)_3, n = (201)_3, m + n = 33 = (1020)_3$ であり，和の計算時に繰り上がりは 2 回発生する．$\binom{33}{14} = 33!/(14!19!) = 818809200 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 23 \cdot 29 \cdot 31$ だから実際に $\deg_3 \binom{33}{14} = 2$ となっている．

証明. Legendre の公式 5.10 から

$$\begin{aligned}
\deg_p \binom{m+n}{m} &= \deg_p \frac{(m+n)!}{m!n!} \\
&= \deg_p (m+n)! - (\deg_p m! + \deg_p n!) \\
&= \sum_{i=1}^{\infty} ((m+n) \operatorname{div} p^i - (m \operatorname{div} p^i + n \operatorname{div} p^i))
\end{aligned}$$

となる．自然数 k に対し，$k \operatorname{div} p^i$ は k の p 進展開の下 i 桁を切り落とした数であるから，

$$(m+n) \operatorname{div} p^i - (m \operatorname{div} p^i + n \operatorname{div} p^i) = 1 \iff i \text{ 桁目で繰り上がりが発生}$$

[*20] $v_p(n), \nu_p(n), \operatorname{ord}_p n$ などの書き方もある．
[*21] de Polignac の公式と呼ぶこともある．

となり，定理の結論を得る． □

命題 5.13. 以下の関係・関数は全て Diophantus 的である．

1. $p < q$ に対し，長さ r の列 $(p, p, \ldots, p)$ の q を底とするコードを返す 3 項関数 $\mathrm{Replicate}(p, q, r)$，
2. $\mathrm{Dominated}(a_1, b_1, a_2, b_2) :\Longleftrightarrow \forall d \geq 1[\mathrm{Elem}(a_1, b_1, d) \leq \mathrm{Elem}(a_2, b_2, d)]$，
3. $\mathrm{PDominated}(a_1, a_2, b) :\Longleftrightarrow \mathrm{Prime}(b) \wedge \mathrm{Dominated}(a_1, b, a_2, b)$，
4. $\mathrm{Bounded}(a, b, c, e) :\Longleftrightarrow \mathrm{Code}(a, b, c) \wedge \forall d \geq 1[\mathrm{Elem}(a, b, d) \leq e]$，
5. $\mathrm{PBounded}(a, b, c, e) :\Longleftrightarrow \mathrm{Prime}(b) \wedge \mathrm{Bounded}(a, b, c, e)$，
6. 三つ組 $(a_1, b_1, c_1), (a_2, b_2, c_2)$ が同じ列のコードであることを表す 6 項関係 $\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2)$，
7. (a, b, c) が「コードが (a_1, b_1, c_1) であるような列」と「コードが (a_2, b_2, c_2) であるような列」を連結した列のコードであることを表す 9 項関係 $\mathrm{Concat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2)$．

証明. 以下のようにすればよい．

1. 等比数列の和の公式より

$$\mathrm{Replicate}(p, q, r) = pq^{r-1} + pq^{r-2} + \cdots + pq + p = \frac{p(1 - q^r)}{1 - q} = p(q^r \dot{-} 1) \operatorname{div} (q \dot{-} 1).$$

3. $\mathrm{PDominated}(a_1, a_2, b)$ が成り立っているときは，$a_1 + (a_2 - a_1) = a_2$ を b 進列として計算したときに繰り上がりは発生しない．一方，ある d について $\mathrm{Elem}(a_1, b, d) > \mathrm{Elem}(a_2, b, d)$ だったとして，$a_1 + (a_2 - a_1) = a_2$ を b 進列として計算すると，d 桁目では $\mathrm{Elem}(a_1, b, d)$ に何かを足してより小さな値 $\mathrm{Elem}(a_2, b, d)$ を作っていることになるが，これは繰り上がりが発生していることに他ならない．よって，Kummer の定理 5.11 より

$$\mathrm{PDominated}(a_1, a_2, b) \iff \mathrm{Prime}(b) \wedge a_1 \leq a_2 \wedge b \nmid \binom{a_2}{a_1}.$$

5. $\mathrm{PBounded}(a, b, c, e) \iff e \geq b \vee \mathrm{PDominated}(a, \mathrm{Replicate}(e, b, c), b)$．
6. いきなり一般の場合を考えるのではなく，まず b_2 が b_1 より十分大きい素数であるような場合を考える．Diophantus 的 6 項関係 $\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2)$ を

$$\begin{aligned}\mathrm{Eq}(a_1, b_1, c_1, a_2, b_2, c_2) \iff{}& \mathrm{Code}(a_1, b_1, c_1) \wedge c_1 = c_2 \wedge \mathrm{PBounded}(a_2, b_2, c_2, b_1 \dot{-} 1) \\ &\wedge b_1^{c_1} + b_1 < b_2 \wedge a_1 \equiv a_2 \pmod{b_2 \dot{-} b_1}\end{aligned}$$

と定義する．

主張 5.14. b_1, c_1, a_2, b_2, c_2 が $c_1 = c_2 \wedge \mathrm{PBounded}(a_2, b_2, c_2, b_1 - 1) \wedge b_1^{c_1} + b_1 < b_2$ を満たすとする．このとき，任意の a_1 に対し

$$\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2) \iff \mathrm{Code}(a_1, b_1, c_1) \wedge a_1 \equiv a_2 \pmod{b_2 - b_1}.$$

主張の証明. $c := c_1 (= c_2)$ とおく．a_2 を列 $(t_1, t_2, \ldots, t_c)$ の cipher とする．すなわち，$a_2 = t_c b_2^{c-1} + \cdots + t_2 b_2^1 + t_1 b_2^0$ である．

($\Longrightarrow$) $\mathrm{Code}(a_1, b_1, c_1)$ が成り立つことは明らか．仮定より a_1 も列 $(t_1, t_2, \ldots, t_c)$ の cipher であるので

$$
\begin{aligned}
a_2 &= t_c b_2^{c-1} + t_{c-1} b_2^{c-2} + \cdots + t_2 b_2^1 + t_1 b_2^0, \\
a_1 &= t_c b_1^{c-1} + t_{c-1} b_1^{c-2} + \cdots + t_2 b_1^1 + t_1 b_1^0, \\
a_2 - a_1 &= t_c (b_2^{c-1} - b_1^{c-1}) + t_{c-1}(b_2^{c-2} - b_1^{c-2}) + \cdots + t_2(b_2^1 - b_1^1) + t_1(b_2^0 - b_1^0)
\end{aligned}
$$

であるが，一般に $k \geq 1$ に対し $b_2^k - b_1^k = (b_2 - b_1)(b_2^{k-1} + b_2 b_1^{k-2} + \cdots + b_2^{k-2} b_1 + b_1^{k-1})$ と因数分解できるので右辺は $b_2 - b_1$ で割り切れる．[*22]よって $a_2 - a_1 \equiv 0 \pmod{b_2 - b_1}$ となる．

左辺を満たす a_1 が存在すること　a_2 の底を b_1 に置き換えた数を $a_1 := t_c b_1^{c-1} + t_{c-1} b_1^{c-2} + \cdots + t_2 b_1^1 + t_1 b_1^0$ とおくと，$\mathrm{PBounded}(a_2, b_2, c_2, b_1 - 1)$ より $\mathrm{Code}(a_1, b_1, c_1)$ が成り立ち，よって $\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2)$ が成り立つ．

右辺を満たす a_1 が高々 1 つであること　まず，$\mathrm{Code}(a_2, b_2, c_2)$ が成り立っていることに注意する．実際，$\mathrm{Code}(a_1, b_1, c_1)$ より $b_1 \geq 2$ だから $b_1^c + b_1 < b_2$ と合わせて $b_2 \geq 2$ であり，また $\mathrm{PBounded}(a_2, b_2, c_2, b_1 - 1)$ から $d \geq c$ に対しては $\mathrm{Elem}(a_2, b_2, d) = 0$ であるから $a_2 < b_2^c$ である．いま $\mathrm{Code}(a_1, b_1, c_1)$ より $a_1 < b_1^{c_1}$ だから，$b_1^{c_1} + b_1 < b_2$ と合わせて $a_1 < b_2 - b_1$ を得る．よって $a_1 \equiv a_2 \pmod{b_2 - b_1}$ と合わせて $a_1 = \mathrm{rem}(a_1, b_2 - b_1) = \mathrm{rem}(a_2, b_2 - b_1)$ を得る．よって右辺を満たす a_1 は存在すればただひとつである．

($\Longleftarrow$)　a_1 が右辺を満たすとする．左辺を満たす a_1' をとると，($\Longrightarrow$) より a_1' は右辺も満たすが，一意性より $a_1 = a_1'$ だから a_1 も左辺を満たす．　□

よって主張 5.14 より $\mathrm{Eq}(a, b, c, x, y, z) \implies \mathrm{Equal}(a, b, c, x, y, z)$ が成り立ち，また素数の無限性から任意のコード (a, b, c) に対しあるコード (x, y, z) が存在して $\mathrm{Eq}(a, b, c, x, y, z)$ となるので，

$$
\mathrm{Equal}(a_1, b_1, c_1, a_2, b_2, c_2) \iff \exists x \exists y \exists z [\mathrm{Eq}(a_1, b_1, c_1, x, y, z) \wedge \mathrm{Eq}(a_2, b_2, c_2, x, y, z)].
$$

2. 底を共通の素数 y に変更すれば

$$
\begin{aligned}
\mathrm{Dominated}(a_1, b_1, a_2, b_2) \iff \exists x_1 \exists x_2 \exists y \exists z [\, &\mathrm{Equal}(a_1, b_1, z, x_1, y, z) \\
&\wedge \mathrm{Equal}(a_2, b_2, z, x_2, y, z) \\
&\wedge \mathrm{PDominated}(a_1, a_2, y)].
\end{aligned}
$$

4. 同様に，$\mathrm{Bounded}(a, b, c, e) \iff \exists x \exists y [\mathrm{Equal}(a, b, c, x, y, c) \wedge \mathrm{PBounded}(x, y, c, e)]$.
7. 底 b_1, b_2 を b に揃えてから比較すれば

$$
\begin{aligned}
\mathrm{Concat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2) \iff \exists x_1 \exists x_2 [\, &\mathrm{Equal}(a_1, b_1, c_1, x_1, b, c_1) \\
&\wedge \mathrm{Equal}(a_2, b_2, c_2, x_2, b, c_2) \\
&\wedge a = x_2 b^{c_1} + x_1 \wedge c = c_1 + c_2].
\end{aligned}
$$

□

5.5　関数の有限列への拡張

以降，本節の終わりまで $b \geq 3$ を固定する．$S_b := \{0, 1, \ldots, b-1\}$ とおく．$F \colon S_b \to S_b$ を任意の関数とする．F は有限集合上の関数なので Diophantus 的である．実際，

$$
y = F(x) \iff (x = 0 \wedge y = F(0)) \vee (x = 1 \wedge y = F(1)) \vee \cdots \vee (x = b-1 \wedge y = F(b-1))
$$

[*22] $b = 0$ の場合も含めて $b^0 = 1$ と約束していたので，$t_1(b_2^0 - b_1^0) = t_1(1 - 1) = 0$ だから 0 次の項も $b_2 - b_1$ で割り切れる．

と書ける．F に対し，関数 $\mathrm{Map}_b(F)\colon \mathbb{N}^2 \to \mathbb{N}$ を次で定義する: 三つ組 (a,b,c) が列 $(a_1,a_2,\ldots,a_c)$ のコードのとき，$\mathrm{Map}_b(F)(a,c)$ を列

$$(F(a_1),F(a_2),\ldots,F(a_c)) \tag{41}$$

の cipher と定める．すなわち，三つ組 $(\mathrm{Map}_b(F)(a,c),b,c)$ が列 (41) のコードになるように定義するということである．

命題 5.15. 任意の $F\colon S_b \to S_b$ に対し，$\mathrm{Map}_b(F)\colon \mathbb{N}^2 \to \mathbb{N}$ は Diophantus 的関数である．

証明のアイデア. 例として $b=4$ で a が $(0,1,2,3,1,1,3,0,2)$ の cipher である場合を考えると，$c=9$ であり

$$a = (203113210)_4$$

である．ここで a の**特性列** (characteristic sequence) h_0,h_1,h_2,h_3 を

$$\begin{aligned} h_0 &:= (010000001)_4,\\ h_1 &:= (000110010)_4,\\ h_2 &:= (100000100)_4,\\ h_3 &:= (001001000)_4 \end{aligned}$$

とおこう．このとき

$$\begin{aligned} h_0+h_1+h_2+h_3 &= (111111111)_4 = \mathrm{Replicate}(1,b,c),\\ 0\cdot h_0 &= (000000000)_4,\\ 1\cdot h_1 &= (000110010)_4,\\ 2\cdot h_2 &= (200000200)_4,\\ 3\cdot h_3 &= (003003000)_4,\\ 0\cdot h_0+1\cdot h_1+2\cdot h_2+3\cdot h_3 &= a \end{aligned}$$

であり

$$\mathrm{Map}_b(F)(a,c) = F(0)\cdot h_0 + F(1)\cdot h_1 + F(2)\cdot h_2 + F(3)\cdot h_3$$

となる．

さて，a から特性列 $h_0,h_1,\ldots,h_{b-1}$ を Diophantus 的関係を用いて計算するにはどうすればよいだろうか．まず，h_i の各桁は 0 か 1 でなければならないが，この条件は

$$\mathrm{Bounded}(h_i,b,c,1)$$

と書ける．次に，$i\neq j$ のときは h_i と h_j の同じ桁が同時に 1 となることはないが，この条件も同様に

$$\mathrm{Bounded}(h_i+h_j,b,c,1)$$

と書ける．さらに，どの d についても h_i の d 桁目が 1 となるような i がなければならないが，この条件は

$$h_0+h_1+\cdots+h_{b-1} = \mathrm{Replicate}(1,b,c)$$

と書ける．ここまでで，各 d に対して，h_i の d 桁目が 1 となるような i がちょうどひとつだけ存在することがわかる．ただし，このままではこの h_i たちは a とは無関係である．よって最後に，条件

$$0 \cdot h_0 + 1 \cdot h_1 + 2 \cdot h_2 + 3 \cdot h_3 = a$$

を課せば h_i たちは晴れて a の特性列となる． □

証明. わかりやすさのために Diophantus 的関係に別名を付ける:

$$\begin{aligned} \mathrm{Normalized}_b(q, r) &:\Longleftrightarrow \mathrm{Bounded}(q, b, r, 1), \\ \mathrm{Orthogonal}_b(q_1, q_2, r) &:\Longleftrightarrow \mathrm{Bounded}(q_1 + q_2, b, r, 1). \end{aligned}$$

このとき，上の議論から y, a, c に関する 3 項関係 $y = \mathrm{Map}_b(F)(a, c)$ は連立 Diophantus 方程式

$$\begin{cases} \bigwedge_{i=0}^{b-1} \mathrm{Normalized}_b(h_i, c), \\ \bigwedge_{0 \le i < j < b} \mathrm{Orthogonal}_b(h_i, h_j, c), \\ \sum_{i=0}^{b-1} h_i = \mathrm{Replicate}(1, b, c), \\ \sum_{i=0}^{b-1} i \cdot h_i = a, \\ y = \sum_{i=0}^{b-1} F(i) \cdot h_i \end{cases}$$

によって定義される． □

次に，今の議論を多変数に拡張することを考えよう．任意の関数 $F\colon S_b^m \to S_b$ に対し，関数 $\mathrm{Map}_b(F)\colon \mathbb{N}^{m+1} \to \mathbb{N}$ を次で定義する: 三つ組 $(a_1, b, c), (a_2, b, c), \ldots, (a_m, b, c)$ がそれぞれ列

$$\begin{gathered} (a_{11}, a_{12}, \ldots, a_{1c}), \\ (a_{21}, a_{22}, \ldots, a_{2c}), \\ \ldots, \\ (a_{m1}, a_{m2}, \ldots, a_{mc}) \end{gathered}$$

のコードであるとき，$\mathrm{Map}_b(F)(a_1, a_2, \ldots, a_m, c)$ を列

$$(F(a_{11}, a_{21}, \ldots, a_{m1}), F(a_{12}, a_{22}, \ldots, a_{m2}), \ldots, F(a_{1c}, a_{2c}, \ldots, a_{mc})) \tag{42}$$

の cipher と定める．すなわち，三つ組 $(\mathrm{Map}_b(F)(a_1, a_2, \ldots, a_m), b, c)$ が列 (42) のコードになるように定義する．

命題 5.16. 任意の $F\colon S_b^m \to S_b$ に対し，$\mathrm{Map}_b(F)\colon \mathbb{N}^{m+1} \to \mathbb{N}$ は Diophantus 的関数である．

証明. 命題 5.15 の証明と同様にして，$a_1, a_2, \ldots, a_m$ に対する特性列を次のように定める: 各 $(i_1, i_2, \ldots, i_m) \in S_b^m$ に対し，$h_{i_1, i_2, \ldots, i_m}$ の d 桁目を，$a_1, a_2, \ldots, a_m$ の d 桁目がそれぞれ $i_1, i_2, \ldots, i_m$ であるとき，またその

ときに限り 1 とする．このようにすれば，同様にして $m+2$ 項関係 $y = \mathrm{Map}_b(F)(a_1, a_2, \ldots, a_m, c)$ は連立 Diophantus 方程式

$$\begin{cases} \bigwedge_{i_1=0}^{b-1} \bigwedge_{i_2=0}^{b-1} \cdots \bigwedge_{i_m=0}^{b-1} \mathrm{Normalized}_b(h_{i_1,i_2,\ldots,i_m}, c), \\ \bigwedge_{(i_1,i_2,\ldots,i_m) \neq (j_1,j_2,\ldots,j_m) \in S_b^m} \mathrm{Orthogonal}_b(h_{i_1,i_2,\ldots,i_m}, h_{j_1,j_2,\ldots,j_m}, c), \\ \sum_{i_1=0}^{b-1} \sum_{i_2=0}^{b-1} \cdots \sum_{i_m=0}^{b-1} h_{i_1,i_2,\ldots,i_m} = \mathrm{Replicate}(1, b, c), \\ \bigwedge_{k=1}^{m} \sum_{i_1=0}^{b-1} \sum_{i_2=0}^{b-1} \cdots \sum_{i_m=0}^{b-1} i_k \cdot h_{i_1,i_2,\ldots,i_m} = a_k, \\ y = \sum_{i_1=0}^{b-1} \sum_{i_2=0}^{b-1} \cdots \sum_{i_m=0}^{b-1} F(i_1, i_2, \ldots, i_m) \cdot h_{i_1,i_2,\ldots,i_m} \end{cases}$$

によって定義される． □

6 c.e. 集合と Diophantus 的集合

本節では計算可能性理論における基本的な対象である c.e. 集合という概念を導入し，c.e. 集合と Diophantus 的集合の関係を記述する MRDP 定理の正確な主張を述べる．MRDP 定理は Hilbert の第 10 問題 HTP($\mathbb{N}$) の決定不能性を系として導く強力かつ一般的な定理であり，本稿での目標となる主定理である．

6.1 c.e. 集合

ここでは自然数 $\mathbb{N}$ 上の部分関数 $\mathbb{N}^n \rightharpoonup \mathbb{N}$ を計算する Turing 機械を用いる．定義については「Turing 機械の変種」[12] を参照のこと．

c.e. 集合の定義に先立って，Turing 機械の s ステップ近似の概念を導入しておく．

定義 6.1. M を部分関数 $\mathbb{N}^n \rightharpoonup \mathbb{N}$ を計算する Turing 機械とする．このとき，M を指定されたステップ数だけ計算する新たな部分関数 $M(-, \ldots, -)[-] \colon \mathbb{N}^{n+1} \rightharpoonup \mathbb{N}$ を次で定義する:

$$M(x_1, \ldots, x_n)[s] := \begin{cases} M(x_1, \ldots, x_n) & M(x_1, \ldots, x_n) \text{ の計算が } s \text{ ステップ以内に停止するとき，} \\ \text{未定義} & M(x_1, \ldots, x_n) \text{ の計算が } s \text{ ステップ以内に停止しないとき．} \end{cases}$$

任意の $x_1, \ldots, x_n, s \in \mathbb{N}$ に対して，$M(x_1, \ldots, x_n)[s]$ の計算結果は (未定義かもしれないが) 有限ステップで求められることに注意する．

命題 6.2. 自然数の集合 $C \subseteq \mathbb{N}$ に対し，次の条件は同値である．

1. $C \neq \emptyset$ かつ，C はある計算可能部分関数 $F_1 \colon \mathbb{N} \rightharpoonup \mathbb{N}$ の定義域 $\mathrm{dom}(F_1) := \{ x \in \mathbb{N} \mid F_1(x)\downarrow \}$ に等しい．
2. C はある (全域的) 計算可能関数 $F_2 \colon \mathbb{N} \to \mathbb{N}$ の値域 $\mathrm{ran}(F_2) := \{ F_2(x) \mid x \in \mathbb{N} \}$ に等しい．

証明. $(1. \Longrightarrow 2.)$ $C = \mathrm{dom}(F_1)$ と仮定し，F_1 を計算する Turing 機械 M_1 をひとつとる．まず，C が有限集合のときは $C = \{c_1, c_2, \ldots, c_n\}$ として計算可能関数 F_2 を以下のようなプログラムによって定めればよい．

Input: x
Output: $F_2(x)$
1: $S \leftarrow \{c_1, c_2, \ldots, c_n\}$
2: **if** $x \in S$ **then**
3: **return** x
4: **else**
5: **return** c_1
6: **end if**

次に C が無限集合と仮定する．このとき，直観的には「$M_1(0), M_1(1), \ldots$ の計算を全て並列に行い，x 番目に停止したものの引数を出力する」ようにすればよい．より具体的には，F_2 を以下のようなプログラムによって定める．

Input: x
Output: $F_2(x)$
1: $S \leftarrow \emptyset$
2: **for all** $s = 0, 1, 2, \ldots$ **do**
3: **for** $i = 0$ **to** s **do**
4: **if** $M_1(i)[s]\downarrow$ **then**
5: $S \leftarrow S \cup \{i\}$
6: **if** $|S| = x + 1$ **then**
7: **return** i
8: **end if**
9: **end if**
10: **end for**
11: **end for**

C が無限集合であることより，F_2 が全域的関数になることがわかる．[*23]

$(2. \Longrightarrow 1.)$ $C = \mathrm{ran}(F_2)$ と仮定し，F_2 を計算する Turing 機械 M_2 をひとつとる．このとき，直観的には「$M_2(0), M_2(1), \ldots$ の値を順に計算し，出力値が x と一致するものがあればその時点で停止する」ようにすればよい．より具体的には，計算可能部分関数 F_1 を以下のようなプログラムによって定める．

Input: x
Output: $F_1(x)$

[*23] ここではわかりやすさのために C が有限集合の場合と無限集合の場合を分けて考えた．ところが，与えられた Turing 機械 M に対して $\mathrm{dom}(M)$ が有限かどうかを判定する問題は決定不能になることが知られている．そのため，ここでの証明は “非一様” である．実は，もう少し工夫をすることで場合分けを回避し，与えられた Turing 機械 M に対し，$(\mathrm{dom}(M) \neq \emptyset$ のときは$)$ $\mathrm{dom}(M) = \mathrm{ran}(M')$ となるような M' を計算可能な形で構成することができる．具体的には，$c \in \mathrm{dom}(M)$ を一つ求めておき (これは $\mathrm{dom}(M) \neq \emptyset$ のときは常に可能である)，入力 x を $x = \mathrm{Cantor}(s, y)$ となるような s, y に分解し，$M(y)[s]\downarrow$ ならば y を，そうでなければ c を返すようにすればよい．

```
1: for all s = 0, 1, 2, ... do
2:   for i = 0 to s do
3:     if M_2(i)[s]↓ = x then
4:       return 1
5:     end if
6:   end for
7: end for
```
□

定義 6.3 (c.e. 集合). 自然数の集合 $C \subseteq \mathbb{N}$ が**計算的枚挙可能集合** (computably enumerable set; c.e. set) [*24]であるとは，$C = \emptyset$ または C が命題 6.2 の条件のいずれか (したがって両方) を満たすことをいう．また，自然数の n 個組の集合 $C' \subseteq \mathbb{N}^n$ が c.e. 集合であるとは，自然数の集合 $\mathrm{Cantor}_n(C') \subseteq \mathbb{N}$ が c.e. 集合であることをいう (これは C' がある Turing 機械 $M\colon \mathbb{N}^n \rightharpoonup \mathbb{N}$ によって $C' = \mathrm{dom}(M)$ と書けることと同値である)．

命題 6.2 の条件 2 より，c.e. 集合は直観的には全ての元をいずれ “並べ上げることができる” ような集合のことである．[*25]しかし，本稿では以降は専ら命題 6.2 の条件 1 の方を用いる．

自然数の集合 $X \subseteq \mathbb{N}$ をひとつ固定すると，X の所属判定問題と呼ばれる決定問題を考えることができる:

問題 6.4 (X の所属判定問題 (membership problem in X)).
Input: 自然数 $x \in \mathbb{N}$
Question: $x \in X$ か？

Turing 機械の停止問題を用いることで，所属判定問題が決定不能となるような c.e. 集合を構成することができる．自然数上の部分関数 $\mathbb{N} \rightharpoonup \mathbb{N}$ を計算する Turing 機械は可算個なので，一列に並べて

$$M_0, M_1, M_2, \ldots$$

と番号を付けておく．本稿では次のバージョンの停止問題を用いる．

問題 6.5 (停止問題 (halting problem)).
Input: 自然数 $e, x \in \mathbb{N}$
Question: $M_e(x)\downarrow$ か？

定理 6.6. 所属判定問題が決定不能となるような c.e. 集合 C が存在する．

証明. 万能 Turing 機械 $U\colon \mathbb{N} \rightharpoonup \mathbb{N}$ を

$$U(\mathrm{Cantor}(e, x)) :\simeq M_e(x)$$

となるように定義する．[*26]このとき，c.e. 集合 $C := \mathrm{dom}(U) \subseteq \mathbb{N}$ の所属判定問題は Turing 機械の停止問題 6.5 と等価だから決定不能である．
□

[*24] 枚挙可能の代わりに可枚挙ということもある．また，**再帰的枚挙可能 (帰納的可算)**(recursively enumerable; r.e.) という用語を使っている本もある．ただ，最近では c.e. 集合と呼ぶのが普通である．

[*25] 実際，c.e. 集合のことを listable set と呼んでいる文献もある．

[*26] U の定義の直観的な説明: まず，任意のプログラム (Turing 機械) を書き表すのに十分なだけのアルファベット Σ を固定する (例えば ASCII の 128 文字があれば十分である)．Σ 上の文字列の全体 Σ^* を長さが短い順に辞書式に並べ，これにより文字列に番

6.2 MRDP 定理の内容

ここまでで c.e. 集合の概念を整備したので，本稿の主定理である MRDP 定理の主張の内容を述べることができる．MRDP 定理は Diophantus 的集合と c.e. 集合が本質的に同じであることを主張する．

定理 6.7 (Matiyasevich-Robinson-Davis-Putnam の定理 (Matiyasevich-Robinson-Davis-Putnam theorem; MRDP theorem)[*27], Matiyasevich, 1970). 自然数の n 個組の集合 $X \subseteq \mathbb{N}^n$ に対し，以下は同値である．

1. X は Diophantus 的集合である．
2. X は c.e. 集合である．

Diophantus 的集合が c.e. 集合であることは簡単にわかる．

(1. $\Longrightarrow$ 2.) の証明. $X \subseteq \mathbb{N}^n$ を多項式 $f(a_1, \ldots, a_n, x_1, \ldots, x_m)$ によって定義される Diophantus 的集合とする．すなわち，

$$X = \{\, (a_1, \ldots, a_n) \in \mathbb{N}^n \mid \exists (x_1, \ldots, x_m) \in \mathbb{N}^m [f(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0] \,\}$$

である．このとき, $\mathrm{dom}(M) = \mathrm{Cantor}_n(X)$ となるような Turing 機械 $M \colon \mathbb{N} \rightharpoonup \mathbb{N}$ を構成したい．直観的には「与えられた $a_1, \ldots, a_n$ に対し，$f(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ となるような $(x_1, \ldots, x_m) \in \mathbb{N}^m$ を探す」ようにすればよい．より具体的には, M を以下のようなプログラムによって定める．

Input: a
Output: $M(a)$

1: $a_1 \leftarrow \mathrm{Elem}_{n,1}(a), \ldots, a_n \leftarrow \mathrm{Elem}_{n,n}(a)$
2: **for all** $s = 0, 1, 2, \ldots$ **do**
3: **for all** $(x_1, \ldots, x_m) \in \{0, 1, \ldots, s\}^m$ **do**
4: **if** $f(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ **then**
5: **return** 1
6: **end if**
7: **end for**
8: **end for**

□

逆向きの証明は次節で行う．

例 6.8. 双子素数全体の集合を $T := \{\, (p, p+2) \mid p \text{ と } p+2 \text{ は素数} \,\} \subseteq \mathbb{N}^2$ とおく．Turing 機械 M を

$$M(a, b) :\simeq \begin{cases} 1 & \mathrm{Prime}(a) \wedge \mathrm{Prime}(b) \wedge a + 2 = b \text{ のとき}, \\ \text{未定義} & \text{それ以外} \end{cases}$$

号を付けて全単射 $\sigma \colon \mathbb{N} \to \Sigma^*$ を作る．このとき，U は次のような動作をするプログラムである: 自然数の組 (e, x) が入力されたら，まず e に対応する文字列 $\sigma(e) \in \Sigma^*$ を求め，$\sigma(e)$ をソースコードとみなして，入力 x に対して $\sigma(e)$ を実行する．ただし，$\sigma(e)$ が妥当なソースコードでなく，コンパイルエラーが発生したときは $U(\mathrm{Cantor}(e, x))$ の値は未定義とする．

[*27] MRDP 定理は DPRM 定理と略されることもある．

とおくと $T = \mathrm{dom}(M)$ であり，したがって命題 6.2 の条件 2 より T は c.e. 集合である．よって，MRDP 定理より T は Diophantus 的である．しかし，双子素数予想は 2018 年現在未解決だから，T が無限集合であるかどうかはわからない．

7　Hilbert の第 10 問題は決定不能である

本節では MRDP 定理を証明し，Hilbert の第 10 問題の決定不能性を確立する．

初めに，証明中の表記を簡潔にするために連結に関する略記法を導入しておく．

定義 7.1.　命題 5.13.7 の 9 項関係 $\mathrm{Concat}(a, b, c, a_1, b_1, c_1, a_2, b_2, c_2)$ をベクトル値関数 $\mathbb{N}^6 \rightharpoonup \mathbb{N}^3$ とみなして

$$(a, b, c) = (a_1, b_1, c_1)^\frown(a_2, b_2, c_2)$$

と略記する．この略記法を用いると，3 つ以上の列の連結 (すなわち，連結の合成) を簡潔に書けるようになる．

それでは MRDP 定理の証明に入ろう．

任意の c.e. 集合 $C \subseteq \mathbb{N}^n$ をとる．c.e. 集合の定義から，自然数値関数を計算するある Turing 機械 $M = (Q, \Gamma, \delta, q_0, q_{\mathrm{halt}})$ が存在して $C = \mathrm{dom}(M)$ となる．このとき，任意の入力 $(a_1, \ldots, a_n) \in \mathbb{N}^n$ に対して，

$$M(a_1, \ldots, a_n)\downarrow \iff \exists x_1 \cdots \exists x_m [f_M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]$$

が成り立つような多項式 $f_M(a_1, \ldots, a_n, x_1, \ldots, x_m)$ を構成したい．

まず，いつものように M はヘッドがテープの左端を見ている状態でさらにヘッドを左に動かそうとすることはないとしてよい．次に，集合の元の名前を自然数で付け替えて $Q = \{1, 2, \ldots, v\}, \Gamma = \{0, 1, \ldots, w\}$ とする．ただし，q_0, q_{halt} はそれぞれ $1, 2 \in Q$ に対応させるものとし，$\llcorner, 1$ はそれぞれ $0, 1 \in \Gamma$ に対応させるものとする．また L, R もそれぞれ $0, 1$ と同一視する．定数 $\beta_M > \max\{2, v, w\}$ を固定する．遷移関数を成分ごとに $\delta(q, \gamma) = (\delta_{\mathrm{state}}(q, \gamma), \delta_{\mathrm{alph}}(q, \gamma), \delta_{\mathrm{dir}}(q, \gamma))$ と書く．つまり，$\delta_{\mathrm{state}} \colon Q \times \Gamma \to Q, \delta_{\mathrm{alph}} \colon Q \times \Gamma \to \Gamma, \delta_{\mathrm{dir}} \colon Q \times \Gamma \to \{\mathrm{L}, \mathrm{R}\}$ である．M の s ステップ目での計算状況 C_s が $\gamma_1 \cdots \gamma_{m-1} q \gamma_m \cdots \gamma_l$ だったとする．つまり，テープの内容が $\gamma_1\gamma_2 \cdots \gamma_l$，状態が q でヘッドが γ_m を見ているとする．このとき，C_s を状態・ヘッドの位置とテープの内容に分けて，長さ l の 2 つの列

$$\begin{aligned}&(0, \ldots, \quad 0 \quad, q, \quad 0 \quad, \ldots, 0),\\ &(\gamma_1, \ldots, \gamma_{m-1}, \gamma_m, \gamma_{m+1}, \ldots, \gamma_l)\end{aligned}$$

の cipher p, t の組 (p, t) によって表す (空白記号$\llcorner$は 0 に対応させることにしていたので，列の長さの情報がなくても問題は生じない)．特に，開始状況 C_0 は

$$\begin{aligned}p_0 &\longleftrightarrow (1, 0, \ldots, 0),\\ t_0 &\longleftrightarrow (\underbrace{1, \ldots, 1}_{a_1+1}, 0, \underbrace{1, \ldots, 1}_{a_2+1}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{a_3+1})\end{aligned} \tag{43}$$

の組 (p_0, t_0) で表される．

まず，M の計算を 1 ステップだけシミュレートすることを考えよう．$C_i = (p_i, t_i)$ から $C_{i+1} = (p_{i+1}, t_{i+1})$ を計算する関数

$$\mathrm{NextPos}_M(p_i, t_i) = p_{i+1},$$
$$\mathrm{NextTape}_M(p_i, t_i) = t_{i+1}$$

を考える．これらの関数がともに Diophantus 的関数であることを示そう．

補題 7.2. 2 項関数 $\mathrm{NextPos}_M(p,t), \mathrm{NextTape}_M(p,t)$ はともに Diophantus 的関数である．[*28]

証明. まず $\mathrm{NextTape}_M(p,t)$ が Diophantus 的であることを示す．有限集合 $S_{\beta_M} = \{0, 1, \ldots, \beta_M - 1\}$ 上の関数 $\delta^{\beta_M}_{\mathrm{alph}} \colon S^2_{\beta_M} \to S_{\beta_M}$ を

$$\delta^{\beta_M}_{\mathrm{alph}}(q,\gamma) = \begin{cases} \delta_{\mathrm{alph}}(q,\gamma) & \text{if } 0 < q \le v, 0 \le \gamma \le w, \\ \gamma & \text{otherwise} \end{cases}$$

と定義する．ここで，$\mathrm{NextTape}_M(p,t)$ (がコードする列) の第 d 成分は p, t (がコードする列) の第 d 成分だけから決まることに注意する．すなわち，

$$\mathrm{Elem}(\mathrm{NextTape}_M(p,t), \beta_M, d) = \delta^{\beta_M}_{\mathrm{alph}}(\mathrm{Elem}(p, \beta_M, d), \mathrm{Elem}(t, \beta_M, d))$$

ということである．したがって，命題 5.16 を用いて $\delta^{\beta_M}_{\mathrm{alph}}$ を有限列上の関数 $\mathrm{Map}_{\beta_M}(\delta^{\beta_M}_{\mathrm{alph}}) \colon \mathbb{N}^3 \to \mathbb{N}$ に拡張すると

$$t' = \mathrm{NextTape}_M(p,t) \iff \exists c[t' = \mathrm{Map}_{\beta_M}(\delta^{\beta_M}_{\mathrm{alph}})(p,t,c)]$$

と書ける．

$\mathrm{NextPos}_M(p,t)$ の方はもう少しやっかいである．なぜかというと，計算状況が C_i から C_{i+1} に遷移するときには必ずヘッドの位置が移動するので，$\mathrm{Elem}(\mathrm{NextPos}_M(p,t), \beta_M, d)$ は $\mathrm{Elem}(p, \beta_M, d), \mathrm{Elem}(t, \beta_M, d)$ だけからは決まらないからである．そこで，次のように p, t (がコードする列) を左右に “ずらした” 列 (のコード) を定める．

$$\begin{array}{rcl} p & \longleftrightarrow & (0, 0, \ldots, \quad 0 \quad , q , \quad 0 \quad , \ldots, \quad 0 \quad , 0), \\ t & \longleftrightarrow & (\gamma_1, \gamma_2, \ldots, \gamma_{m-1}, \gamma_m, \gamma_{m+1}, \ldots, \gamma_{l-1}, \gamma_l), \\ p^{\mathrm{L}} & \longleftrightarrow & (0, 0, \ldots, q , \quad 0 \quad , \quad 0 \quad , \ldots, 0, 0), \\ t^{\mathrm{L}} & \longleftrightarrow & (\gamma_2, \gamma_3, \ldots, \gamma_m, \gamma_{m+1}, \gamma_{m+2}, \ldots, \gamma_l, 0), \\ p^{\mathrm{R}} & \longleftrightarrow & (0, 0, \ldots, \quad 0 \quad , \quad 0 \quad , q , \ldots, \quad 0 \quad , \quad 0 \quad , 0), \\ t^{\mathrm{R}} & \longleftrightarrow & (0, \gamma_1, \ldots, \gamma_{m-2}, \gamma_{m-1}, \gamma_m, \ldots, \gamma_{l-2}, \gamma_{l-1}, \gamma_l). \end{array}$$

具体的には

$$p^{\mathrm{L}} = p \operatorname{div} \beta_M, \qquad p^{\mathrm{R}} = p\beta_M,$$
$$t^{\mathrm{L}} = t \operatorname{div} \beta_M, \qquad t^{\mathrm{R}} = t\beta_M$$

と書ける．関数 $\delta^{\beta_M}_{\mathrm{pos}} \colon S^4_{\beta_M} \to S_{\beta_M}$ を

$$\delta^{\beta_M}_{\mathrm{pos}}(q^{\mathrm{L}}, q^{\mathrm{R}}, \gamma^{\mathrm{L}}, \gamma^{\mathrm{R}}) = \begin{cases} \delta_{\mathrm{state}}(q^{\mathrm{L}}, \gamma^{\mathrm{L}}) & \text{if } 0 < q^{\mathrm{L}} \le v, 0 \le \gamma^{\mathrm{L}} \le w, \delta_{\mathrm{dir}}(q^{\mathrm{L}}, \gamma^{\mathrm{L}}) = \mathrm{L}, \\ \delta_{\mathrm{state}}(q^{\mathrm{R}}, \gamma^{\mathrm{R}}) & \text{if } 0 < q^{\mathrm{R}} \le v, 0 \le \gamma^{\mathrm{R}} \le w, \delta_{\mathrm{dir}}(q^{\mathrm{R}}, \gamma^{\mathrm{R}}) = \mathrm{R}, \\ 0 & \text{otherwise} \end{cases}$$

[*28] ただし，(p,t) が計算状況を表していないようなときの値は何であってもよい (未定義でもよいし，対応する値が複数あってもよい) とする．

と定義する．再び命題 5.16 を用いて $\delta_{\mathrm{pos}}^{\beta_M}$ を有限列上の関数 $\mathrm{Map}_{\beta_M}(\delta_{\mathrm{pos}}^{\beta_M})\colon \mathbb{N}^5 \to \mathbb{N}$ に拡張すると

$$p' = \mathrm{NextPos}_M(p,t) \iff \exists c[p' = \mathrm{Map}_{\beta_M}(\delta_{\mathrm{pos}}^{\beta_M})(p \operatorname{div} \beta_M, p\beta_M, t \operatorname{div} \beta_M, t\beta_M, c)]$$

と書ける． □

次に，$\mathrm{NextPos}_M(p,t), \mathrm{NextTape}_M(p,t)$ を 1 ステップから k ステップにそれぞれ拡張した関数 $\mathrm{AfterPos}_M(k,p,t), \mathrm{AfterTape}_M(k,p,t)$ を考える．すなわち，帰納的に

$$\begin{aligned}
\mathrm{AfterPos}_M(0,p,t) &:= p,\\
\mathrm{AfterTape}_M(0,p,t) &:= t,\\
\mathrm{AfterPos}_M(k+1,p,t) &:= \mathrm{NextPos}_M(\mathrm{AfterPos}_M(k,p,t), \mathrm{AfterTape}_M(k,p,t)),\\
\mathrm{AfterTape}_M(k+1,p,t) &:= \mathrm{NextTape}_M(\mathrm{AfterPos}_M(k,p,t), \mathrm{AfterTape}_M(k,p,t))
\end{aligned}$$

と定義するということである．

補題 7.3. $k > 0$ に対し，3 項関数 $\mathrm{AfterPos}_M(k,p,t), \mathrm{AfterTape}_M(k,p,t)$ は Diophantus 的である．

証明のアイデア. Diophantus 方程式で再帰的定義を直接書くことはできないことに注意する．$0, 1, \ldots, k$ ステップ目の計算状況をそれぞれ $(p,t) = (p_0,t_0), (p_1,t_1), \ldots, (p_k,t_k) = (p',t')$ とおく．まず，k ステップをシミュレートするのに必要なテープの長さ l を求める．k ステップの間に追加で使用することができるテープの長さは高々 k マスだから，l は計算開始時のテープの長さより k マス以上長ければ十分である．よって，$\beta_M^{l-k-2} > \max\{p,t\}$ となるように l をとれば，各 $i = 0, 1, \ldots, k$ について $\beta_M^{l-2} > \max\{p_i, t_i\}$ となる．補題 7.2 の証明から，$\mathrm{NextTape}_M(p,t)$ や $\mathrm{NextPos}_M(p,t)$ の第 d 成分は p,t の第 $d-1$ 成分，第 d 成分，第 $d+1$ 成分だけから決まる，いわば “局所的” な条件であることがわかる．よって，各計算状況を

$$\begin{aligned}
(P_{\mathrm{bef}}, \beta_M, kl) &= (p_0,\beta_M,l)^\frown(p_1,\beta_M,l)^\frown\cdots^\frown(p_{k-1},\beta_M,l),\\
(T_{\mathrm{bef}}, \beta_M, kl) &= (t_0,\beta_M,l)^\frown(t_1,\beta_M,l)^\frown\cdots^\frown(t_{k-1},\beta_M,l),\\
(P_{\mathrm{aft}}, \beta_M, kl) &= \qquad (p_1,\beta_M,l)^\frown\cdots^\frown(p_{k-1},\beta_M,l)^\frown(p_k,\beta_M,l),\\
(T_{\mathrm{aft}}, \beta_M, kl) &= \qquad (t_1,\beta_M,l)^\frown\cdots^\frown(t_{k-1},\beta_M,l)^\frown(t_k,\beta_M,l)
\end{aligned}$$

のように連結して，正しい遷移になっているかどうかを

$$\begin{aligned}
P_{\mathrm{aft}} &= \mathrm{NextPos}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}}),\\
T_{\mathrm{aft}} &= \mathrm{NextTape}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}})
\end{aligned}$$

として 1 回だけ検査すればよい (図 6).

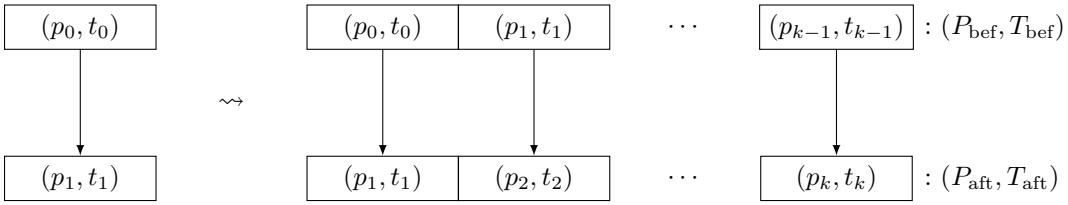


図 6: 局所的な検査を一斉に行う

ただし，Diophantus 方程式のパラメーターの個数は k によらない定数でなければならないので，実際には中間の計算状況は

$$\begin{aligned}(P_{\mathrm{int}},\beta_M,(k-1)l)&=(p_1,\beta_M,l)^\frown\cdots^\frown(p_{k-1},\beta_M,l),\\(T_{\mathrm{int}},\beta_M,(k-1)l)&=(t_1,\beta_M,l)^\frown\cdots^\frown(t_{k-1},\beta_M,l)\end{aligned}\tag{44}$$

のようにしてそれぞれ 1 つの変数 $P_{\mathrm{int}},T_{\mathrm{int}}$ にまとめておく． □

証明. $p'=\mathrm{AfterPos}_M(k,p,t)$ かつ $t'=\mathrm{AfterTape}_M(k,p,t)$ となることは，$l,P_{\mathrm{bef}},T_{\mathrm{bef}},P_{\mathrm{int}},T_{\mathrm{int}},P_{\mathrm{aft}},T_{\mathrm{aft}}$ を未知数とする連立 Diophantus 方程式

$$\begin{cases}\beta_M^l>p\beta_M^{k+2},\\ \beta_M^l>t\beta_M^{k+2},\\ (P_{\mathrm{bef}},\beta_M,kl)=(p,\beta_M,l)^\frown(P_{\mathrm{int}},\beta_M,(k\dot{-}1)l),\\ (T_{\mathrm{bef}},\beta_M,kl)=(t,\beta_M,l)^\frown(T_{\mathrm{int}},\beta_M,(k\dot{-}1)l),\\ (P_{\mathrm{aft}},\beta_M,kl)=(P_{\mathrm{int}},\beta_M,(k\dot{-}1)l)^\frown(p',\beta_M,l),\\ (T_{\mathrm{aft}},\beta_M,kl)=(T_{\mathrm{int}},\beta_M,(k\dot{-}1)l)^\frown(t',\beta_M,l),\\ P_{\mathrm{aft}}=\mathrm{NextPos}_M(P_{\mathrm{bef}},T_{\mathrm{bef}}),\\ T_{\mathrm{aft}}=\mathrm{NextTape}_M(P_{\mathrm{bef}},T_{\mathrm{bef}})\end{cases}$$

が解を持つことと同値であることを示す．命題 5.13.6 と同様の手法で証明する．(p,t) が計算状況を表しているような任意の k,p,t をとる．さらに，$\beta_M^{l-k-2}>\max\{p,t\}$ を満たすような l を (存在するので) 1 つとる．このとき，任意の $p',t',P_{\mathrm{bef}},T_{\mathrm{bef}},P_{\mathrm{int}},T_{\mathrm{int}},P_{\mathrm{aft}},T_{\mathrm{aft}}$ に対し，

$$\begin{cases}p'=\mathrm{AfterPos}_M(k,p,t),\\ t'=\mathrm{AfterTape}_M(k,p,t)\end{cases}\iff\begin{cases}(P_{\mathrm{bef}},\beta_M,kl)=(p,\beta_M,l)^\frown(P_{\mathrm{int}},\beta_M,(k\dot{-}1)l),\\ (T_{\mathrm{bef}},\beta_M,kl)=(t,\beta_M,l)^\frown(T_{\mathrm{int}},\beta_M,(k\dot{-}1)l),\\ (P_{\mathrm{aft}},\beta_M,kl)=(P_{\mathrm{int}},\beta_M,(k\dot{-}1)l)^\frown(p',\beta_M,l),\\ (T_{\mathrm{aft}},\beta_M,kl)=(T_{\mathrm{int}},\beta_M,(k\dot{-}1)l)^\frown(t',\beta_M,l),\\ P_{\mathrm{aft}}=\mathrm{NextPos}_M(P_{\mathrm{bef}},T_{\mathrm{bef}}),\\ T_{\mathrm{aft}}=\mathrm{NextTape}_M(P_{\mathrm{bef}},T_{\mathrm{bef}})\end{cases}$$

となることを示せばよい．

($\Longrightarrow$) 仮定から計算状況の列 $(p,t)=(p_0,t_0),(p_1,t_1),\dots,(p_k,t_k)=(p',t')$ が存在する．このとき式 (44) のようにして中間の計算状況を $P_{\mathrm{int}},T_{\mathrm{int}}$ にまとめれば右辺の解が得られる．

左辺を満たす p',t' が存在すること $\mathrm{AfterPos}_M,\mathrm{AfterTape}_M$ の定義から明らかに左辺を満たす p',t' がただひとつ存在する．[*29]

右辺を満たす $p',t',P_{\mathsf{bef}},T_{\mathsf{bef}},P_{\mathsf{int}},T_{\mathsf{int}},P_{\mathsf{aft}},T_{\mathsf{aft}}$ が高々 1 つであること $p=0$ は計算状況を表していないので $p\geq1$ だから，$p\geq1,k\geq1,\beta_M^{l-k-2}>p$ より $l>3$ であることに注意する．まず，$P_{\mathrm{bef}},T_{\mathrm{bef}}$ の最初の l 個の成分はそれぞれ p,t だから一意に定まっている．次に，$\mathrm{NextPos}_M,\mathrm{NextTape}_M$ の値は局所的な情報だけから決まるのだったから，$P_{\mathrm{aft}}=\mathrm{NextPos}_M(P_{\mathrm{bef}},T_{\mathrm{bef}}),T_{\mathrm{aft}}=\mathrm{NextTape}_M(P_{\mathrm{bef}},T_{\mathrm{bef}})$ より $P_{\mathrm{aft}},T_{\mathrm{aft}}$ の，したがって $P_{\mathrm{int}},T_{\mathrm{int}}$ の最初の $(l-1)$ 個の成分も一意に定まる．このとき $P_{\mathrm{bef}},T_{\mathrm{bef}}$ の最初の $(2l-1)$ 個の成分が決まっていることになるので，$l<2l-1$ であることと M が「ヘッドがテープの左端を見ているときにさらにヘッドを左に動かそうとすることはない」という条件を満たすことを合わせ

[*29] ただし，途中で状態が q_{halt} になっても計算を続けるものと考える．

ると，$\delta_{\mathrm{pos}}^{\beta_M}$ の定義から $P_{\mathrm{int}}, T_{\mathrm{int}}$ の第 l 成分も一意に決まる．再び $P_{\mathrm{aft}} = \mathrm{NextPos}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}}), T_{\mathrm{aft}} = \mathrm{NextTape}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}})$ を用いると $P_{\mathrm{int}}, T_{\mathrm{int}}$ の最初の $(2l-1)$ 個の成分が一意に定まり，よって $P_{\mathrm{bef}}, T_{\mathrm{bef}}$ の最初の $(3l-1)$ 個の成分が決まっていることになるので，$2l < 3l-1$ より $P_{\mathrm{int}}, T_{\mathrm{int}}$ の第 $2l$ 成分も一意に決まる．同様の推論を繰り返すことで，結局 $P_{\mathrm{int}}, T_{\mathrm{int}}$ の $(k-1)l$ 個の成分全てが一意に定まることになる．最後に再び $P_{\mathrm{aft}} = \mathrm{NextPos}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}}), T_{\mathrm{aft}} = \mathrm{NextTape}_M(P_{\mathrm{bef}}, T_{\mathrm{bef}})$ を用いると p', t' の l 個の成分が全て一意に定まる．

($\Longleftarrow$) 右辺の解をひとつとると，左辺を満たす p', t' から定まる右辺の解と等しくなければならず，したがって左辺を満たす． □

ここまでの議論をまとめると，M の停止性を表現する Diophantus 方程式が得られる．

定理 6.7 の証明. $M(a_1, \ldots, a_n)\downarrow$ となることは，p, t, k, r を未知数とする連立 Diophantus 方程式

$$\begin{cases} p = 1, & (45.1) \\ (t, \beta_M, a_1 + \cdots + a_n + 2n \dot{-} 1) \\ \qquad = (\mathrm{Replicate}(1, \beta_M, a_1 + 1), \beta_M, a_1 + 1)^\frown(0, \beta_M, 1) \\ \qquad\quad {}^\frown(\mathrm{Replicate}(1, \beta_M, a_2 + 1), \beta_M, a_2 + 1)^\frown(0, \beta_M, 1) \\ \qquad\quad {}^\frown \cdots {}^\frown(0, \beta_M, 1)^\frown(\mathrm{Replicate}(1, \beta_M, a_n + 1), \beta_M, a_n + 1), & (45.2) \\ \mathrm{Elem}(\mathrm{AfterPos}_M(k, p, t), \beta_M, r) = 2 & (45.3) \end{cases}$$

が解を持つことと同値である．実際，式 (45.1)，(45.2) は開始状況を表す式 (43) そのものであり，また q_{halt} を $2 \in Q$ に対応させていたことから，式 (45.3) を満たす k, r が存在することと $M(a_1, \ldots, a_n)$ の計算が停止することは同値である． □

MRDP 定理 6.7 から HTP($\mathbb{N}$) が決定不能になることが導かれるが，万能 Turing 機械を用いるとより強いことがわかる．

系 7.4. HTP($\mathbb{N}; n, d$) が決定不能となるような n, d が存在する．

証明. 定理 6.6 より，所属判定問題が決定不能になるような c.e. 集合 $C = \mathrm{dom}(U) \subseteq \mathbb{N}$ がとれる．このとき MRDP 定理 6.7 より C はある Diophantus 方程式 $f_U(a, x_1, \ldots, x_m) = 0$ によって定義される．よって，与えられた自然数 $a \in \mathbb{N}$ に対し，$f_U(a, x_1, \ldots, x_m) = 0$ となるような $(x_1, \ldots, x_m) \in \mathbb{N}^m$ が存在するかどうかは決定不能だから，$n := m, d := \deg f_U$ とおけば HTP($\mathbb{N}; n, d$) が決定不能になる． □

注意 7.5. 系 7.4 から，任意の Diophantus 方程式の解の存否は f_U の解の存否に帰着されることが言える．実際，任意の Diophantus 方程式 $g(y_1, \ldots, y_n) = 0$ に対し，g の解を探索する Turing 機械 $M_{e(g)}$ を

$$M_{e(g)}(x) :\simeq \begin{cases} 1 & \exists y_1 \cdots \exists y_n [g(y_1, \ldots, y_n) = 0], \\ \text{未定義} & \text{それ以外} \end{cases}$$

と定義すれば，[*30]

$$\begin{aligned} \exists y_1 \cdots \exists y_n [g(y_1, \ldots, y_n) = 0] &\iff M_{e(g)}(0)\downarrow \\ &\iff U(\mathrm{Cantor}(e(g), 0))\downarrow \\ &\iff \exists x_1 \cdots \exists x_m [f_U(\mathrm{Cantor}(e(g), 0), x_1, \ldots, x_m) = 0] \end{aligned}$$

[*30] 正確には，このように定義した Turing 機械の**指標** (index) を $e(g)$ とおく，ということである．

となる．このことから，Diophantus 方程式 $f_U(a, x_1, \ldots, x_m) = 0$ を**万能 Diophantus 方程式** (universal Diophantine equation) と呼ぶ．

本節の手法による万能 Diophantus 方程式の構成は Turing 機械を経由したいくぶん間接的なものであるが，実際には「Diophantus 方程式のコード化」の技法を開発することにより万能 Diophantus 方程式を直接構成することができる [1, Chapter 4]．

8 MRDP 定理以後

本節では，MRDP 定理から導かれる様々な系や，第 10 問題の変種，また $\mathrm{HTP}(\mathbb{N}; n, d)$ の決定可能性の境界や，その他の環 A における $\mathrm{HTP}(A)$ の決定不能性などについて述べる．本節では証明や定義の多くを省略する．詳細についてはそれぞれの文献を参照してほしい．

8.1 Hilbert の第 10 問題の副産物

ここでは，第 10 問題の決定不能性から導かれるいくつかの結果を紹介する．

8.1.1 素数を表す多項式

以下のように，素数の値のみをとる非自明な多項式関数は，かなり緩い条件のもとであっても存在しないことが知られている．

命題 8.1 ([1, Exercise 1.5]). 素数の値のみをとる多項式であって，2 つ以上の素数の値をとる多項式関数 $f\colon \mathbb{Z} \to \mathbb{Z}$ は存在しない．さらに強く，以下の条件であっても存在しない:

- 素数の定義を緩めて，負の素数 $-2, -3, -5, \ldots$ を素数に含めたとしても存在しない．
- f を多変数多項式 $f \in \mathbb{Z}[x_1, \ldots, x_n]$ に拡張して，$f\colon \mathbb{Z}^n \to \mathbb{Z}$ としても存在しない．
- f の定義域を自然数 $\mathbb{N}^n$ に制限して $f\colon \mathbb{N}^n \to \mathbb{Z}$ としても存在しない．

証明. $f(x_1, \ldots, x_n)$ を素数の値のみをとる多項式関数とする．$p := |f(0, \ldots, 0)|$ とおく．このとき，任意の $(y_1, \ldots, y_n) \in \mathbb{N}^n$ に対し，

$$f(py_1, \ldots, py_n) \equiv f(0, \ldots, 0) \equiv 0 \pmod{p}$$

が成り立つ．f は素数の値しかとらないので $f(py_1, \ldots, py_n) = \pm p$ は定数多項式となり，したがって $f(x_1, \ldots, x_n)$ も定数である． □

ところが，任意の Diophantus 的集合はある多項式関数の値域の正の部分に等しいということを示すことができる．正の整数全体を $\mathbb{Z}_{>0} := \{\, n \in \mathbb{Z} \mid n > 0 \,\}$ とおく．

命題 8.2. 0 を含まない任意の (1 次元の) Diophantus 的集合 $D \subseteq \mathbb{Z}_{>0}$ に対し，ある多変数多項式 $F(x_0, \ldots, x_n) \in \mathbb{Z}[x_0, \ldots, x_n]$ が存在して

$$D = \{\, F(x_0, \ldots, x_n) \in \mathbb{Z} \mid (x_0, \ldots, x_n) \in \mathbb{N}^{n+1} \,\} \cap \mathbb{Z}_{>0}$$

が成り立つ．

証明. D が多項式 $f(a, x_1, \ldots, x_n)$ によって定義されているとする．このとき，任意の $a > 0$ に対し

$$\exists x_1 \cdots \exists x_n [f(a, x_1, \ldots, x_n) = 0] \iff \exists x_0 \exists x_1 \cdots \exists x_n [x_0(1 - f(x_0, x_1, \ldots, x_n)^2) = a]$$

となるので，$F(x_0, x_1, \ldots, x_n) := x_0(1 - f(x_0, x_1, \ldots, x_n)^2)$ とおけばよい． □

よって，系 5.8 より素数全体の集合は Diophantus 的集合だったから，値域の正の部分が素数全体に一致するような多項式が存在することになる．そのような多項式としてどれだけ簡単なものがとれるか，ということについては次の結果が知られている．

定理 8.3 (Jones-Sato-Wada-Wiens [13], 1976). 26 変数多項式 $M(a, b, \ldots, z)$ を

$$\begin{aligned}
(k+2)\{1 &- [wz + h + j - q]^2 \\
&- [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
&- [2n + p + q + z - e]^2 \\
&- [16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\
&- [e^3(e+2)(a+1)^2 + 1 - o^2]^2 \\
&- [(a^2 - 1)y^2 + 1 - x^2]^2 \\
&- [16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\
&- [n + l + v - y]^2 \\
&- [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
&- [(a^2 - 1)l^2 + 1 - m^2]^2 \\
&- [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
&- [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2 \\
&- [ai + k + 1 - l - i]^2 \\
&- [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2\}
\end{aligned}$$

で定義すると，集合 $\{ M(a, b, \ldots, z) \in \mathbb{Z} \mid (a, b, \ldots, z) \in \mathbb{N}^{26} \} \cap \mathbb{Z}_{>0}$ は素数全体の集合に一致する．

証明については原論文 [13] の他に INTEGERS [14] なども参照のこと．

8.1.2 有界量化記号の消去

3 節では Diophantus 的関係が $\wedge, \vee, \exists$ といった論理演算について閉じていることを見た．一方で，Diophantus 的関係は全称量化記号 $\forall$ については閉じていない．しかし，MRDP 定理を用いると，Diophantus 的関係が弱い全称量化については閉包性を持つことが示せる．

命題 8.4. Diophantus 的関係は**有界全称量化記号** (bounded universal quantifier) $\forall x < a$ について閉じている．すなわち，$R(a_1, \ldots, a_n)$ を Diophantus 的 n 項関係とするとき，n 項関係

$$\forall x < a_n [R(a_1, \ldots, a_{n-1}, x)]$$

も Diphantus 的である．方程式の言葉で書けば，

$$R(a_1, \ldots, a_n) \iff \exists x_1 \cdots \exists x_m [f(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]$$

であるとき，

$$\forall x < a_n \exists x_1 \cdots \exists x_m [f(a_1, \ldots, a_{n-1}, x, x_1, \ldots, x_m) = 0] \tag{46}$$

は Diophantus 的関係である．

証明. 任意の整数係数多項式 $f(a_1, \ldots, a_n, x_1, \ldots, x_m)$ に対し，Turing 機械 M を以下のプログラムによって定める．

Input: $a_1, \ldots, a_n$
Output: $M(a_1, \ldots, a_n)$

```
1: for all s = 0, 1, 2, ... do
2:   for all (x_1, ..., x_m) ∈ {0, 1, ..., s}^m do
3:     b ← 1
4:     for x = 0 to a_n − 1 do
5:       if f(a_1, ..., a_{n−1}, x, x_1, ..., x_m) ≠ 0 then
6:         b ← 0
7:       end if
8:     end for
9:     if b = 1 then
10:      return 1
11:    end if
12:  end for
13: end for
```

このとき，$M(a_1, \ldots, a_n)\downarrow \iff \forall x < a_n \exists x_1 \cdots \exists x_m [f(a_1, \ldots, a_{n-1}, x, x_1, \ldots, x_m) = 0]$ となるから関係 (46) で定まる Diophantus 的集合はは c.e. 集合である．よって，MRDP 定理 6.7 より $\mathrm{dom}(M)$ は Diophantus 的集合である．すなわち，ある整数係数多項式 $g(a_1, \ldots, a_n, y_1, \ldots, y_l)$ が存在して

$$\exists y_1 \cdots \exists y_l [g(a_1, \ldots, a_n, y_1, \ldots, y_l) = 0] \iff \forall x < a_n \exists x_1 \cdots \exists x_m [f(a_1, \ldots, a_{n-1}, x, x_1, \ldots, x_m) = 0]$$

となる． □

系 8.5. $R(a_1, \ldots, a_n)$ を Diophantus 的 n 項関係，F を Diophantus 的 1 項関数とするとき，n 項関係

$$\forall x < F(a_n)[R(a_1, \ldots, a_{n-1}, x)]$$

は Diophantus 的である．

証明. 明らかに

$$\forall x < F(a_n)[R(a_1, \ldots, a_{n-1}, x)] \iff \exists y [y = F(a_n) \wedge \forall x < y [R(a_1, \ldots, a_{n-1}, x)]$$

だから，$\forall x < y[R(a_1, \ldots, a_{n-1}, x)]$ を $(a_1, \ldots, a_{n-1}, y)$ をパラメーターとみなして命題 8.4 を適用することで有界量化記号を消去すればよい． □

注意 8.6. ここでの有界全称量化記号消去の証明は Turing 機械を経由した間接的なものであるが，実際には中国剰余定理を利用したコード化 (Gödel コード化) によって有界全称量化記号のない方程式を直接的に構成することもできる [1, Section 6.2].

8.1.3　Goldbach 予想と Diophantus 方程式

Goldbach 予想とは「4 以上の任意の偶数は 2 つの素数の和で書ける」という主張であり，これは 2018 年現在未解決である．先程の有界全称量化記号の消去を用いると，Goldbach 予想がある Diophantus 方程式の解の非存在と同値になることが示せる．

定理 8.7.　非可解性が Goldbach 予想と同値になるような Diophantus 方程式が存在する．

証明. Goldbach 予想が成り立たないと仮定すると，2 つの素数の和で書けないような 4 以上の偶数 $2a+4$ $(a \geq 2)$ が存在する．$2a+4$ を 2 つの 2 以上の自然数の和に分けると，少なくとも一方は $(2a+4)/2 = a+2$ 以下だから，小さい方を $z+2$ $(0 \leq z \leq a)$ とおけば，$z+2$ と $2a+4-(z+2)$ の少なくとも一方は合成数である．すなわち，

$$\forall z < a+1 \exists x \exists y [z+2 = (x+2)(y+2) \vee 2a+4-(z+2) = (x+2)(y+2)] \tag{47}$$

となる．系 8.5 より，ある整数係数多項式 $f(a, x_1, \ldots, x_m)$ が存在して論理式 (47) は

$$\exists x_1 \cdots \exists x_m [f(a, x_1, \ldots, x_m) = 0]$$

と同値である．よって，Goldbach 予想は

$$\neg \exists x_0 \exists x_1 \cdots \exists x_m [f(x_0, x_1, \ldots, x_m) = 0]$$

と同値である．　□

さらに，補題 2.3 の証明と同様の議論により，Goldbach 予想はある方程式の整数解の非存在と同値であることもわかる．

8.1.4　Riemann 予想と Diophantus 方程式

coming soon

8.1.5　Gödel の不完全性定理と Diophantus 方程式

coming soon

8.2　HTP の変種

coming soon

8.3　決定可能・決定不能の境界

coming soon

8.4　その他の環における結果

coming soon

参考文献

[1] Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, 1993.

[2] 杉浦光夫 (編), ヒルベルト 23 の問題, 日本評論社, 1997.

[3] ヒルベルトの第 1 0 問題 - Sendai Logic Homepage, https://sites.google.com/site/sendailogichomepage/files/ref/ref_05.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduation Texts in Mathematics, Vol. 138, Springer-Verlag, New York, 1993, https://doi.org/10.1007/978-3-662-02945-9.

[5] 吉永正彦, 周期と実数の 0-認識問題 —Kontsevich-Zagier の予想—, 数学書房, 2016.

[6] @mod_poppo, 週刊 代数的実数を作る, https://miz-ar.info/math/algebraic-real/.

[7] 雪江明彦, 整数論 1 初等整数論から p 進数へ, 日本評論社, 2013.

[8] A. Shlapentokh, *Hilbert's Tenth Problem: Diophantine Classes and Other Extensions to Global Fields*, Cambridge University Press, 2007.

[9] 廣瀬健, 帰納的関数, 共立出版, 1989.

[10] M. Davis, Hilbert's Tenth Problem is Unsolvable, *Amer. Math. Monthly* **80** no. 3 (1973) 233–269, https://doi.org/10.2307/2318447.

[11] y., Cantor の対関数の全単射性の証明 (2016), http://iso.2022.jp/math/pairing_function.pdf.

[12] y., Turing 機械の変種 (2018), http://iso.2022.jp/math/undecidable-problems/files/variants-of-turing-machine.pdf.

[13] J. Jones, D. Sato, H. Wada, D. Wiens, Diophantine Representation of the Set of Prime Numbers, *Amer. Math. Monthly* **83** (1976) 449–464, https://www.maa.org/programs/maa-awards/writing-awards/diophantine-representation-of-the-set-of-prime-numbers.

[14] せきゅーん, 素数とは A〜Z で見つけられる数である (証明編) - INTEGERS (2016), http://integers.hatenablog.com/entry/2016/09/08/010024.

変更履歴

2018/12/20　公開