

離散数学

— 3. 数学的帰納法 —

3.1 数学的帰納法

3.2 再帰の定義

3.1 数学的帰納法

定理 1. $M \subseteq \mathbb{N} = \{1, 2, 3, \dots\}$ とする。

もし, M が次の条件

1. $1 \in M,$

2. $\forall k \in \mathbb{N} : [k \in M \Rightarrow k + 1 \in M]$

を満たすならば, $M = \mathbb{N}$ である。

(証明の方針) 対偶を用いる。

$M \neq \mathbb{N}$ を仮定すると, 条件 1 と 2 は同時に成立しないことを示す.

i) $1 \notin M$ ならば 条件 1 “ $1 \in M$ ” が成立しない。

ii) $1 \in M$ とする. 差集合 $\mathbb{N} - M$ の最小値を m とすれば,

$m \in \mathbb{N}$ かつ $m \notin M$ かつ $m - 1 \in M \subseteq \mathbb{N}$ である. すなわち,

条件 2 “ $m - 1 \in \mathbb{N} : [m - 1 \in M \Rightarrow m \in M]$ ” が成立しない. ■

定理 2. (数学的帰納法 I)

P を $\mathbb{N}$ 上で定義された述語, $P : \mathbb{N} \longrightarrow \{T, F\}$, とする。

もし、次の条件 1, 2 が成り立つならば, $\forall n \in \mathbb{N} : P(n)$ である。

1. $P(1)$,

2. $\forall k \in \mathbb{N} : [P(k) \Rightarrow P(k + 1)]$

(証明) 条件 1, 2 が成立するとする. $M := \{n \in \mathbb{N} \mid P(n)\} (\subset \mathbb{N})$ とする。

条件 1 より、 $P(1)$ が成立するから, $1 \in M$.

さらに、条件 2 と M の定義より、任意の $k \in \mathbb{N}$ に対し、

$$k \in M \Rightarrow P(k) \Rightarrow P(k + 1) \Rightarrow k + 1 \in M.$$

したがって、前記の定理より, $M = \mathbb{N}$.

ゆえに、任意の $k \in \mathbb{N}$ に対し, $k \in M$ であるから $P(n)$ が成り立つ. ■

1. を 帰納法の基礎, 2. を 帰納ステップ, 2. の $P(k)$ を 帰納法の仮定

例 3.

連続する 3 つの自然数の 3 乗の和は, 9 で割り切れることを、
数学的帰納法 I を用いて証明せよ。

(証明) 自然数 n に対し, $f(n) = n^3 + (n+1)^3 + (n+2)^3$ とする。

命題 $P(n)$ を $P(n) = “ f(n) は 9 で割り切れる ”$ とする。

1. (帰納法の基礎) $1 \in \mathbb{N}$ に対し, $f(1) = 1^3 + 2^3 + 3^3 = 36 = 4 \times 9$ より,
 $P(1)$ は成り立つ。

2. (帰納ステップ) 自然数 k に対し, $P(k)$ が成り立つと仮定する (帰納法の
仮定). このとき, $P(k+1)$ について調べる。

$$\begin{aligned} f(k+1) &= (k+1)^3 + (k+2)^3 + \underline{(k+3)^3} \\ &= (k+1)^3 + (k+2)^3 + \underline{k^3 + 9k^2 + 27k + 27} \\ &= \underline{k^3 + (k+1)^3 + (k+2)^3} + 9(k^2 + 3k + 3) \\ &= \underline{P(k)} + 9(k^2 + 3k + 3) \end{aligned}$$

これより, $f(k+1)$ は 9 で割り切れ, $P(k+1)$ が成り立つ。

以上より, 数学的帰納法 I より, 任意の自然数 n に対し, $P(n)$ は成り立つ。 ■

数学的帰納法 I では,

$n = 1$ において $P(n)$ が真であること

を確かめ, その後,

すべての自然数 n に対して $P(n)$ が真であること

を導いた.

しかし, 帰納法の基礎において, 常に $n = 1$ とする必要はなく,

一般の整数でも成り立つ. そのことを次の定理にて示す。

定理 5. (**数学的帰納法 II**) $n_0 \in \mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ を任意に固定した整数とし, P を n_0 以上の整数に対して定義された述語とする.

もし, 次の条件 1, 2 が成り立つならば, $\forall n \geq n_0 : P(n)$ である.

1. $P(n_0)$,

2. $\forall k \geq n_0 : [P(k) \Rightarrow P(k+1)]$

(**証明**) $n := m - 1 + n_0$ とすると, $Q(m) := P(m - 1 + n_0)$ は,

$\mathbb{N}$ 上で定義された述語となる. ($m = 1, 2, \dots$)

そして, 条件 1, 2 が成立するならば,

1'. $Q(1) = P(n_0)$ より, $Q(1)$ は真.

2'. $Q(k) = P(k - 1 + n_0)$ かつ $Q(k+1) = P((k+1) - 1 + n_0)$. そして,

$P(k - 1 + n_0) \Rightarrow P((k+1) - 1 + n_0)$ より $Q(k) \Rightarrow Q(k+1)$.

したがって, 数学的帰納法 I より, $\forall m \in \mathbb{N} : Q(m)$ が成り立つ.

すなわち, $\forall n \geq n_0 : P(n)$ が成り立つ. ■

例 6.

3 円と 4 円の切手だけで 6 円以上の任意の郵便代金を支払えることを数学的帰納法 II を用いて証明せよ.

(証明) $f(a, b) = 3a + 4b$ とする.

1. $k = 6 (= n_0)$ のとき, $(a, b) = (2, 0)$ とすれば $f(2, 0) = 6$.

2. $k \geq 6$ に対し, $f(a_1, b_1) = k$ となる (a_1, b_1) が存在すると仮定する.

このとき, $k + 1$ に対しても $f(a_2, b_2) = k + 1$ となる (a_2, b_2) が存在することを示す.

ここで, $(a, b) = (3, -2) = (-1, 1)$ のとき, $f(a, b) = 1$ に注意する.

i. $a_1 = 0$ のとき, $4b_1 = k \geq 6$ より, $b_1 \geq 2$. したがって、

$$\begin{aligned} k + 1 &= f(a_1, b_1) + f(3, -2) = 3a_1 + 4b_1 + 3 \cdot 3 + 4 \cdot (-2) \\ &= 3(a_1 + 3) + 4(b_1 - 2) = f(a_1 + 3, b_1 - 2). \end{aligned}$$

このとき, $a_1 + 3 \geq 0$ かつ $b_1 - 2 \geq 0$ より,

$(a_2, b_2) = (a_1 + 3, b_1 - 2)$ とすれば $f(a_2, b_2) = k + 1$ となる.

ii. $a_1 > 0$ のとき,

$$k + 1 = f(a_1, b_1) + f(-1, 1) = f(a_1 - 1, b_1 + 1).$$

このとき, $a_1 - 1 \geq 0$ かつ $b_1 + 1 \geq 0$ より,

$(a_2, b_2) = (a_1 - 1, b_1 + 1)$ とすれば $f(a_2, b_2) = k + 1$ となる.

以上のことより, 数学的帰納法 II より, 3 円と 4 円の切手だけで 6 円以上の任意の郵便代金を支払えることが示された. ■

6 以上の任意の整数 n に対し,

$$f(a, b) = n$$

を満たす非負整数の組 (a, b) が存在する.

注意 7.

一般に、互いに素な整数 x, y と非負整数 a, b に対し、
整数 $(x-1)(y-1)$ 以上のすべての整数を $a \cdot x + b \cdot y$ のかたち
で表現できる。■

下線部分のプリント要訂正: $(a-1)(b-1) \rightarrow (x-1)(y-1)$

$$(3-1)(4-1) = 2 \times 3 = 6$$

例 8.

50 円と 70 円の切手だけで 240 円以上の任意の郵便代金を支払えることを証明せよ。
ただし、代金は 10 円単位とする。

~~$(50-10)(70-1) = 40 \times 60 = 240$~~ 訂正
 $(5-1)(7-1) = 4 \times 6 = 24$

定理 9. (数学的帰納法 III)

P を $\mathbf{N}$ 上で定義された述語とする.

もし、次の条件 1, 2 が成り立つならば、 $\forall n \in \mathbf{N} : P(n)$ である.

1. $P(1)$,

2. $\forall k \in \mathbf{N} : [(1 \leq \forall \ell \leq k : P(\ell)) \Rightarrow P(k + 1)]$

(定理の主張)

(数学的帰納法 I) : $\forall n \in \mathbf{N} : P(n)$

「 $P(k)$ が成り立つならば、 $P(k + 1)$ も成り立つ」

(数学的帰納法 III) : $\forall n \in \mathbf{N} : P(n)$

「 $P(1), P(2), \dots, P(k)$ が成り立つならば、 $P(k + 1)$ も成り立つ」

例 10.

数列 $a_1, a_2, \dots$ を $a_1 = 1, \quad a_n = \sum_{k=1}^{n-1} a_k + 1 \quad (n \geq 2)$ と定義する. 任意の自然数 n に対し, $a_n = 2^{n-1}$ が成り立つことを数学的帰納法 III により証明せよ。

(証明)

i. $n = 1$ のとき, $a_n = a_1 = 1 = 2^0 = 2^{n-1}$ より, 等式が成り立つ.

ii. $k = 1, 2, \dots, n$ のすべての k に対し, $a_k = 2^{k-1}$ が成り立つと仮定する.

そして, $n + 1$ の場合に, $a_{n+1} = 2^{(n+1)-1} = 2^n$ が成り立つことを示す.

$$a_{n+1} = \sum_{k=1}^n a_k + 1 = \sum_{k=1}^n 2^{k-1} + 1 = (2^0 + 2^1 + \dots + 2^{n-1}) + 1 = \frac{(1 - 2^n)}{1 - 2} + 1 = 2^n$$

(Handwritten red annotations: a circle around a_k in the sum, an arrow pointing to a_k from below, and the text "訂正 $a^k \rightarrow a_k$ " with a red arrow pointing to the circle.)

以上のことより、数学的帰納法 III より、任意の自然数 n に対し、 $a_n = 2^{n-1}$ が成り立つ。■

ヒント: $(x^0 + x^1 + x^2 + \dots + x^{n-1})(1 - x) = 1 - x^n$

例 11.

任意の自然数 a, r に対し, a から始まる連続する r 個の整数の積 $a(a+1)(a+2)\cdots(a+r-1)$ は $r!$ で割り切れる.

$5 \times 4 \times 3 (= 60)$ は $3! = 3 \times 2 \times 1 (= 6)$ で割り切れる.

例 12.

n 個の中から r 個を取り出す組合せの総数

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-(r-1))}{r!} = \frac{n!}{r! \cdot (n-r)!}$$

は常に **整数値** となる.

$$\binom{5}{3} = \frac{5 \times 4 \times 3}{3 \times 2 \times 1} = \frac{5 \times 4 \times 3 \times 2 \times 1}{(3 \times 2 \times 1)(2 \times 1)} = 10$$

3.2 再帰的定義

定義 13. (再帰的定義)

ある種の集合は、次のように再帰的に定義できる。

1. (初期ステップ) 集合 S の要素なるものを幾つか列挙する。
2. (再帰ステップ) S の要素であることが分かっているものを用いて、 S の新たな要素を定義する。
3. (限定句) 上記の 1, 2 で定まるものだけが S の要素であることを述べる。(この条件は、省略することが多い)

例 14. (再帰的定義)

次のように再帰的に定義される集合 S はどのような集合であるか。

1. A さんを S の要素とする。
2. x さんが S の要素ならば、 x さんの子供を S の要素とする。
3. 上記の 1, 2 で定まるものだけを S の要素とする。

(解答)

1 より、 A さんは S に含まれる。

2 より、 A さんの子供はすべて S に含まれる。

さらに、 A さんの子供の子供も S に含まれる。

これが繰り返される。

3 より、上記以外の人 S には含まない。

以上より、集合 S は A さんの子孫の全体からなる集合である。■

定義 15. ある種の関数 $f : \mathbb{N} \longrightarrow \mathbb{N}$ は、次のように再帰的に定義できる.

1. (**初期ステップ**) 幾つかの関数の値 $f(1), f(2), \dots, f(m)$ を列挙する。
2. (**再帰ステップ**) $n > m$ に対し、 $f(k), 1 \leq k \leq m$ の中の幾つかを用いて $f(n)$ を定義する。

再帰的定義の例として、次の階乗の関数や漸化式があげられる。

例 16. (再帰的定義)

1. (階乗) 関数 $f(n) = n!$, $n \in \mathbb{N}$ は、次のように定義される。

i. $f(1) = 1,$

ii. $f(n) = nf(n-1), n \geq 2$

このとき, $a_n = f(n)$ とすれば,

数列 $a_1, a_2, a_3, a_4, \dots$ は, $1, 2, 6, 24, \dots$ となる.

2. (等差数列) 数列 $a_1, a_2, a_3, \dots$, は、次のように定義される。

i. $a_1 = 3,$

ii. $a_{n+1} = a_n + 2, n \geq 1$

このとき, 数列 $a_1, a_2, a_3, a_4, \dots$ は, $3, 5, 7, 9, \dots$ となる.

これは公差 2 の等差数列で, $a_n = 3 + 2(n-1)$ と書ける.

3. (フィボナッチ数 (Fibonacci number))

数列 $a_0, a_1, a_2, a_3, \dots$ は、次のように定義される。

i. $a_0 = 0, a_1 = 1,$

ii. $a_n = a_{n-1} + a_{n-2}, \quad n \geq 2$

このとき、数列 $a_0, a_1, a_2, a_3, a_4, a_5, a_6, \dots$ は、

$0, 1, 1, 2, 3, 5, 8, \dots$

となる。

ファイボナッチ数列の第 n 項 a_n はどのように書き表されるか。

例 17. (**フィボナッチ数列** (*Fibonacci number*))

下記の再帰式で定義される数列を **フィボナッチ数列** という。

i. $a_0 = 0, a_1 = 1,$

ii. $a_n = a_{n-1} + a_{n-2}, \quad n \geq 2$

この再帰式に対し、多項式 $X^2 - X - 1$ を その特性多項式という。

この多項式の 2 根を α, β ($\alpha > \beta$) とすると、

ファイボナッチ数列の第 n 項は

$$a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$$

と表されることを数学的帰納法を用いて証明せよ。

ここで、 $X^2 - X - 1$ の根である α, β について、

$$\alpha + \beta = 1, \alpha\beta = -1$$

であり、また、解の公式より、 $X = \frac{1 \pm \sqrt{5}}{2}$. ($\alpha = \frac{1 + \sqrt{5}}{2}, \beta = \frac{1 - \sqrt{5}}{2}$).

(証明) $(\alpha + \beta = 1, \alpha\beta = -1)$

1. $n = 0$ のとき, $a_0 = 0 = \frac{1}{\sqrt{5}}(\alpha^0 - \beta^0)$.

$n = 1$ のとき, $a_1 = 1 = \frac{1}{\sqrt{5}}(\alpha^1 - \beta^1)$.

2. n のとき, $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ は正しいと仮定する.

このとき, $n + 1$ についても正しいことを示す。

$$\begin{aligned}\alpha^{n+1} - \beta^{n+1} &= (\alpha^n - \beta^n)(\alpha + \beta) - \alpha\beta(\alpha^{n-1} - \beta^{n-1}) \\ &= \sqrt{5}a_n(\alpha + \beta) - \alpha\beta\sqrt{5}a_{n-1} \\ &= \sqrt{5}a_n + \sqrt{5}a_{n-1} = \sqrt{5}(a_n + a_{n-1}) \\ &= \sqrt{5}a_{n+1}.\end{aligned}$$

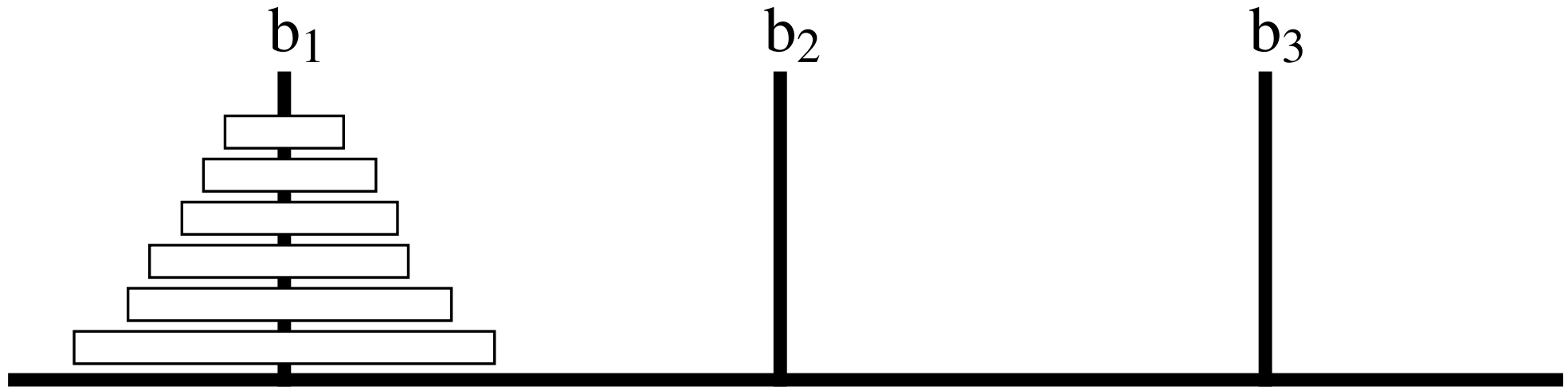
ゆえに, $a_{n+1} = \frac{1}{\sqrt{5}}(\alpha^{n+1} - \beta^{n+1})$ が成り立つ。

以上より, 数学的帰納法より, 0 を含む 任意の自然数 n について

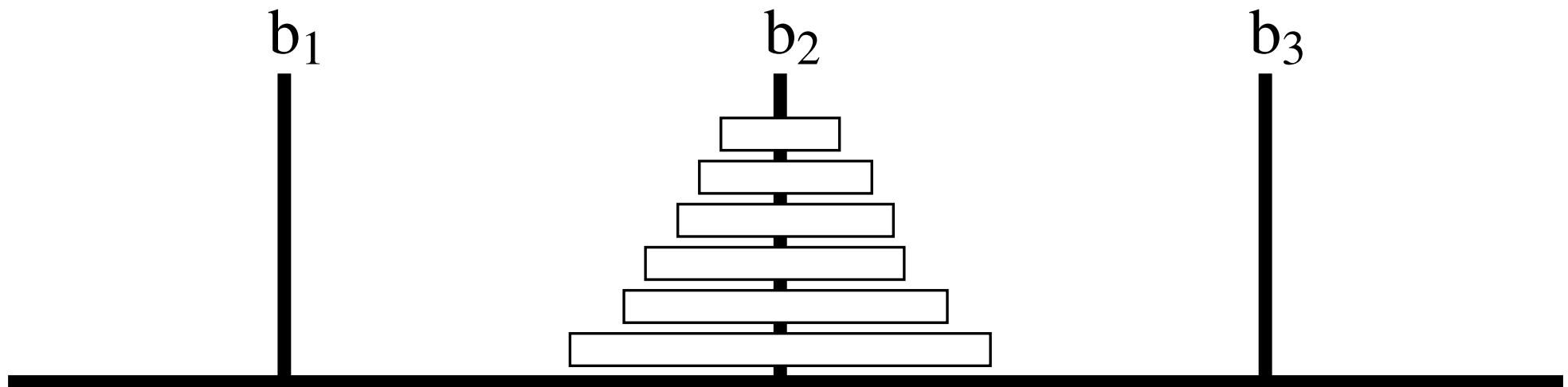
$$a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n) \text{ が成り立つ。} \blacksquare$$

例 18. (ハノイの塔 (*Tower of Hanoi*))

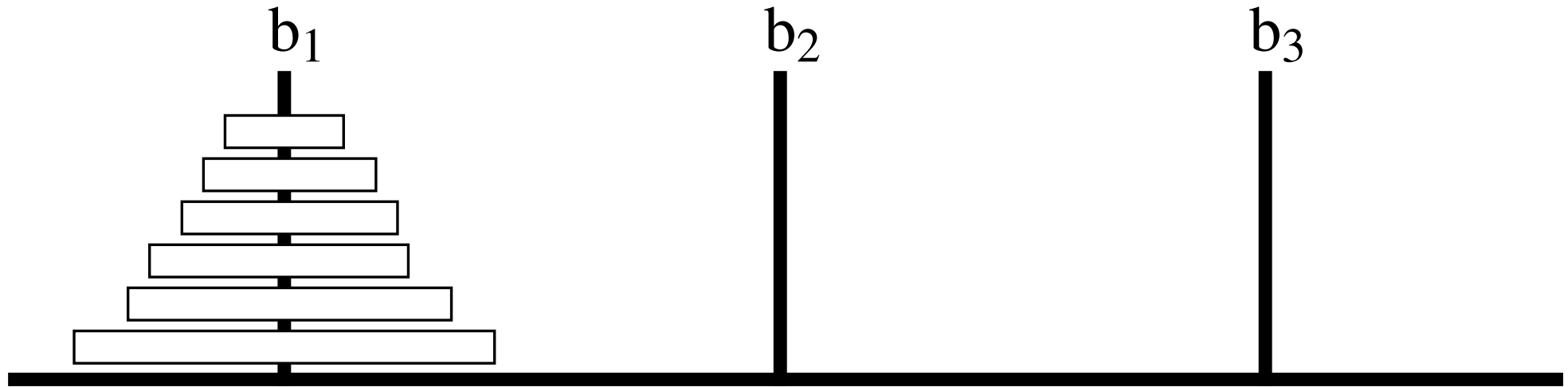
はじめ



おわり



(ハノイの塔 (Tower of Hanoi))



1. n 個の円盤を移し終えるために必要な操作回数を $f(n)$ とするとき,
 $f(n)$ と $f(n-1)$ の間の再帰的な関係を求めよ.
2. $f(n)$ が n のどのような関数になるかを予想し,
それを数学的帰納法で証明せよ.

(証明) n 個の円盤を小さい順に $D_1, D_2, \dots, D_{n-1}, D_n$ とする.

1. i. $n - 1$ 個の円盤 $D_1, \dots, D_{n-1}$ を棒 b_1 から b_3 に移す. $f(n - 1)$ 回

ii. 一番大きい円盤 D_n を棒 b_1 から b_2 に移す. 1 回

iii. $n - 1$ 個の円盤 $D_1, \dots, D_{n-1}$ を棒 b_3 から b_2 に移す. $f(n - 1)$ 回

ゆえに,

$$f(n) = 2f(n - 1) + 1.$$

2.

n		$f(n)$	$f(n) - f(n - 1)$
1	$1 =$	1	
2	$2 \times 1 + 1 =$	3	$2 = 2^1$
3	$2 \times 3 + 1 =$	7	$4 = 2^2$
4	$2 \times 7 + 1 =$	15	$8 = 2^3$
5	$2 \times 15 + 1 =$	31	$16 = 2^4$

これより,

$$f(n) = \sum_{k=1}^{n-1} 2^k + 1, \quad n \geq 1$$

と推測される。さらに, $f(n)$ を整理し、

$$f(n) = \frac{2^n - 2}{2 - 1} + 1 = 2^n - 1$$

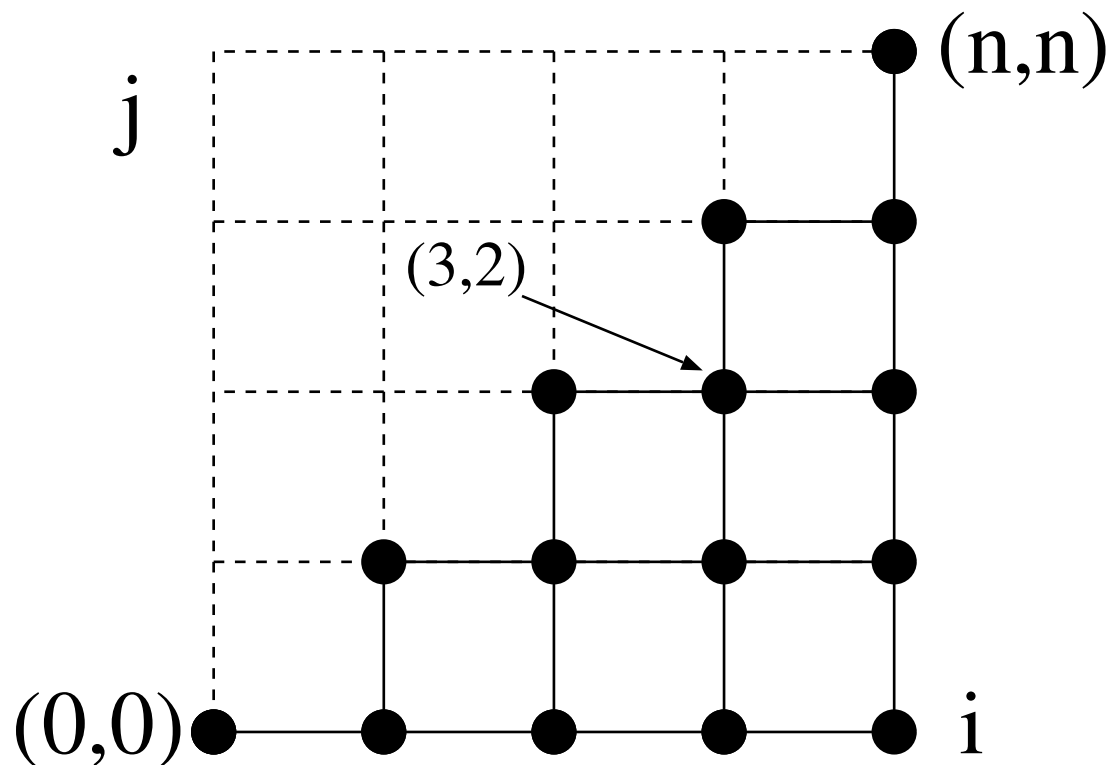
となる。

あとは, これが正しいことを、数学的帰納法を用いて示せばよい. ■

$$f(n) = \frac{2^n - 2}{2 - 1} + 1 = 2^n - 1$$

n	$f(n) = 2^n - 1$	
10	$2^{10}/(60) = 17.066666667$	約 17 分
20	$2^{20}/(60 * 60 * 24) = 12.1362963$	約 12 日
25	$2^{25}/(60 * 60 * 24 * 365) = 1.064004059$	約 1 年
30	$2^{30}/(60 * 60 * 24 * 365) = 34.04812988$	約 34 年

例 19. (**カタラン数 (Catalan numbers)**) カタラン数 C_n は、図のような $n \times n$ の格子上において、格子点 $(0,0)$ から (n,n) へ至る最短経路の総数である。ただし、図の実線部分のみが利用できる経路である。



1. カタラン数 C_n は、次のような再帰的な関係をもつことを示せ。

$$C_0 = 1, C_1 = 1, C_n = \sum_{k=1}^n C_{k-1} C_{n-k}.$$

2. カタラン数 C_n は、 $C_n = \frac{1}{n+1} \binom{2n}{n}$ と表されることを示せ。

References

- [1] 尾関和彦, (情報技術者のための) 離散系数学入門, 共立出版, 2004.
- [2] 尾関和彦, 太田和夫, 國廣昇, “離散数学第一” 及び “離散数学第一演習問題集” 電気通信大学情報通信工学科講義資料, 2004.
- [3] 松坂和夫, 集合・位相入門, 岩波書店, 2003.
- [4] 松坂和夫, 代数系入門, 岩波書店, 2003.
- [5] *S. Lipschutz* 著, 成嶋弘監訳, 離散数学 (コンピュータサイエンスの基礎数学), オーム社, 2004(H16).
- [6] 小倉久和, 情報の基礎離散数学 (— 演習を中心とした —), 近代科学社, 2006.
- [7] 町田元, 横森貴, 計算機数学, 森北出版, 1990.