整数論的な命題の組合せ論的証明

縫田 光司

2023 年 6 月 7 日（初版）

概要

非負整数に関する等式を「同一の濃度（要素数）をもつ有限集合の要素たちを二通りの方法で数え上げる」という手法で示す証明を組合せ論的証明と呼ぶ。このノートでは、いくつかの整数論的な命題について組合せ論的な証明を記す。

記号について

正整数全体の集合を $\mathbb{Z}_{>0}$ で表し、非負整数全体の集合を $\mathbb{Z}_{\geq 0}$ で表す。$n, m \in \mathbb{Z}$ について $[n, m] := \{k \in \mathbb{Z} \mid n \leq k \leq m\}$ と定める。集合 S と $n \in \mathbb{Z}_{\geq 0}$ について、S の n 元部分集合全体の集合を $\binom{S}{n}$ で表す。つまり $\binom{S}{n} = \{T \subseteq S : |T| = n\}$ である。$n \in \mathbb{Z}_{>0}$ と $a, b \in \mathbb{Z}$ について、$a \equiv b \pmod{n}$ を $a \equiv_n b$ で表す。また、$a \in \mathbb{Z}$ を $n \in \mathbb{Z}_{>0}$ で割った余りを $a \bmod n$ で表す。

1　準備体操：二項係数の表示

まずは、組合せ論的証明という手法自体の例示として、二項係数の具体的表示の証明を述べる。ここで、非負整数 $n, m \in \mathbb{Z}_{\geq 0}$ について二項係数 $\binom{n}{m}$ を、n 個の要素からなる集合（例えば集合 $[1, n]$）の m 元部分集合の個数と定義する。冒頭で準備した記号を用いると、$\binom{n}{m} = |\binom{[1,n]}{m}|$ とも表せる。これは定義より直ちに非負整数である。この二項係数は以下のように表せるのであった。この事実の組合せ論的な証明を述べる。なお、定義より $m > n$ であれば $\binom{n}{m} = 0$ であることを注意しておく。

命題 1. $n, m \in \mathbb{Z}_{\geq 0}$, $m \leq n$ のとき $\displaystyle\binom{n}{m} = \frac{n!}{m!(n-m)!}$ である。

証明. n 次対称群 S_n（つまり、1 から n までの整数の並べ方全体の集合）の要素たちを二通りの方法で数え上げる。まず、n 個の数字全体について、先頭にくる数字は n 通り、次にくる数字は $n-1$ 通り、その次は $n-2$ 通り、という具合に数え上げると、$|S_n| = n!$ が得られる。

一方で、(i) 先頭から m 番目までにくる m 個の数字の集合 I を先に選んでおき、(ii) I の要素たちを 1 番目から m 番目までに並べて、(iii) I の要素以外を $m+1$ 番目から n 番目までに並べる、という方法でも S_n の要素を過不足なく数え上げられる。(i) での I の選び方は二項係数の定義より $\binom{n}{m}$ 通りである。その各々について、(ii) での並べ方は、m 個の数字の並べ方であるから、前段落の議論より $m!$ 通りである。同様に (iii) での並べ方は、数字が $n-m$ 個あるので $(n-m)!$ 通りである。よって、(ii) と (iii) の並べ方は I をどう選んでもそれぞれ $m!(n-m)!$ 通りであるから、全体では $\binom{n}{m} \cdot m!(n-m)!$ 通りである。

この二通りの数え上げ方から、$n! = |S_n| = \binom{n}{m} \cdot m!(n-m)!$ となり、両辺を $m!(n-m)!$ で割ることで主張の等式が得られる。 □

2　Fermat の小定理

Fermat の小定理の主張は以下の通りである（いくつか等価な表現があるが下記はその一つである）。

定理 1 (Fermat の小定理)**.** p を素数とすると、$a \in \mathbb{Z}$ について $a^p \equiv_p a$ である。

これは初等整数論の有名な結果の一つであり、有限体 $\mathbb{F}_p$ の乗法群を用いる群論的証明や、$(a+1)^p$ の展開式を用いた数学的帰納法による証明などが良く知られている。ここではこの定理の組合せ論的な証明を述べる。

証明. 合同式の性質より、a を $a + kp$（$k \in \mathbb{Z}$）に変えても左辺や右辺を p で割った余りは変化しない。そのため $a > 0$ と仮定して差し支えない。主張を示すには、$a^p - a$ が p の倍数であることを示せばよい。

X を $[1, a]^p$、つまり、1 から a までの整数を p 個並べた列全体の集合とする。このとき $|X| = a^p$ である。

一方で、列 $x = (x_1, x_2, \ldots, x_{p-1}, x_p) \in X$ の成分を巡回的にずらして $\sigma(x) = (x_2, x_3, \ldots, x_p, x_1) \in X$ にする操作 σ を考える。$\sigma^p(x) = x$ であることを注意しておく（σ^k は σ を k 回続けて施すことを表す）。この σ を何回か施して移り合う列たちをひとまとめにした部分集合を考えたい。その準備として、X に属する列 x たちは「$\sigma(x) = x$ である」（1 型と呼ぶ）か「$k \in [1, p-1]$ について $\sigma^k(x) \neq x$ である」（2 型と呼ぶ）のどちらかを満たすことを示す（なお、$p \geq 2$ であるから、両方を満たすことはない）。どちらも満たさない $x \in X$ があると仮定すると、x は 2 型でないことから、ある $k \in [1, p-1]$ について $\sigma^k(x) = x$ となる。このような最小の k を選んでおく。x は 1 型でもないので $2 \leq k \leq p-1$ である。p は素数であるから、k は p の約数ではなく、p を k で割り算して $p = qk + r$, $q \in \mathbb{Z}_{\geq 0}$, $r \in [1, k-1]$ と表せる。すると、k の選び方より $\sigma^k(x) = x$ であるので、$\sigma^{qk}(x) = x$ となる。また、$\sigma^p(x) = \sigma^{qk+r}(x) = x$ である。これらを比較すると $\sigma^r(x) = x$ となるが、$1 \leq r < k$ であるから、これは k の最小性に反する。よって X の要素は 1 型か 2 型のいずれかである。

$x \in X$ が 1 型であることは、x の成分がすべて等しいということであり、そのような x は全部で a 個ある。よって 2 型である X の要素は全部で $a^p - a$ 個ある。一方で $x \in X$ が 2 型のとき、$\sigma(x)$ も 2 型であり、集合 $[x] := \{\sigma^k(x) \mid k \in [0, p-1]\}$ は p 個の異なる要素からなる（もし $k < \ell$ かつ $\sigma^k(x) = \sigma^\ell(x)$ であれば、成分を σ と逆向きに k 回ずらすことで $x = \sigma^{\ell-k}(x)$ となるが、x は 2 型であるから矛盾する）。よって、$[x]$ という形の X の部分集合を二つとると、互いに一致するか交わりをもたないかのいずれかである。このことから、2 型である X の要素全体の集合は、$[x]$ という形の互いに交わらない部分集合たちに分割できる。各 $[x]$ は p 個の要素をもつので、2 型である X の要素の個数 $a^p - a$ は p の倍数である。よって主張が成り立つ。　□

注意 1. 代数学の言葉を用いて上記の証明を簡潔に説明すると、σ が生成する位数 p の巡回群の集合 X への作用について、X の軌道分解を考えると、各軌道のサイズは 1 または p であり、サイズ 1 をもつ軌道は全部で a 個あるため、$|X| - a$ は p の倍数となる。以降でもこうした群作用による軌道分解の考え方を用いる。

3　二項係数の約数の性質

命題 2. $n, m \in \mathbb{Z}_{>0}$ について、n と m が互いに素であれば $\binom{n}{m}$ は n の倍数である。

この命題の特別な場合として、p が素数であり $k \in [1, p-1]$ であれば $\binom{p}{k}$ は p の倍数である、という有名な事実が得られる。なお、2 節で少し触れた $(a+1)^p$ の展開式を用いた数学的帰納法による Fermat の小定理の証明ではこの事実を用いるが、前述の組合せ論的な証明ではこの事実を用いなかったことを注意しておく。

証明. $X := \binom{[1,n]}{m}$ と定める。二項係数の定義より $|X| = \binom{n}{m}$ である。

写像 $\sigma\colon [1,n] \to [1,n]$ を、$\sigma(k) := k+1$（$1 \le k \le n-1$）および $\sigma(n) := 1$ で定める。つまり σ は長さ n の巡回置換 $(1\ 2\ \cdots\ n) \in S_n$ である。$S = \{s_1, \ldots, s_m\} \in X$ について $\widehat{\sigma}(S) := \{\sigma(s_1), \ldots, \sigma(s_m)\}$ として操作 $\widehat{\sigma}$ を定める。σ が置換であることから $\widehat{\sigma}(S) \in X$ であることを注意しておく。また $\widehat{\sigma}^n$ は恒等変換 id である。この $\widehat{\sigma}$ を繰り返し施して移り合う X の要素たちをひとまとめにする分解（つまり、群 $\langle\widehat{\sigma}\rangle$ の作用による軌道分解）を考えると、各部分（軌道）は n 個以下の要素からなる。これらがすべてちょうど n 個の要素からなることを示せば、全体集合 X の要素数 $|X| = \binom{n}{m}$ が n の倍数であることが示されて証明が完了する。そのため、以下では要素数が n 個未満の軌道があると仮定して矛盾を導く。この軌道は $S \in X$ に $\widehat{\sigma}$ を繰り返し施して得られたものであるとする。

この軌道の要素数が n 個未満であるので、ある $k \in [1, n-1]$ について $\widehat{\sigma}^k(S) = S$ が成り立つ。このような最小の k を選んでおく。特に、S の各要素 a について $\sigma^k(a) \in S$ である。n を k で割り算して $n = qk + r$, $q \in \mathbb{Z}_{\ge 0}$, $r \in [0, k-1]$ と表すと、$a \in S$ について、σ の定義より $\sigma^n(a) = a$ であるから、$\sigma^{n+k-r}(a) = \sigma^{k-r}(a)$ である。一方で $n + k - r = (q+1)k$ であり、k の選び方より $\sigma^k(S) \subseteq S$ であるから、$\sigma^{n+k-r}(a) \in S$ となる。よって $\sigma^{k-r}(a) \in S$ である。すると $\widehat{\sigma}^{k-r}(S) = S$ となり、$r > 0$ のときこれは k の最小性に反するので、$r = 0$、したがって k は n の約数である。$\tau := \sigma^k$, $d := n/k$ とすると、$\tau^d = \sigma^n = \mathsf{id}$ である。さらに、$a \in S$, $\ell \in [1, d-1]$ のとき、$1 \le k \cdot \ell < n$ であるから、σ の定義より $\tau^\ell(a) = \sigma^{k\cdot\ell}(a) \neq a$ である。よって、S の要素たちを τ を繰り返し施して移り合う要素たちのなす部分（つまり、群 $\langle\tau\rangle$ の作用による軌道）に分解すると、各軌道はちょうど d 個の要素からなり、したがって $|S|$ は d の倍数である。しかし、$|S| = m$ は n と互いに素であり、d は n の約数かつ $d > 1$ であるから、これは矛盾である。以上で証明が完了した。 □

なお、命題 2 の逆は成り立たない。例えば $\binom{10}{4} = \frac{10\cdot 9\cdot 8\cdot 7}{4\cdot 3\cdot 2\cdot 1} = 210$ がその反例を与える。

4 Lucas の定理

初等整数論における Lucas の定理 [1] は以下の主張である。ここではその組合せ論的な証明を与える。

定理 2 (Lucas の定理)**.** p を素数とする。$d \in \mathbb{Z}_{>0}$ とし、$n, m \in \mathbb{Z}_{\ge 0}$ は p 進法で d 桁以内で表せるとする。その表示を $n = (n_{d-1}n_{d-2}\cdots n_0)_p$, $m = (m_{d-1}m_{d-2}\cdots m_0)_p$ とする（$n_i, m_i \in [0, p-1]$ であり、最上位桁が 0 でも構わない）。このとき

$$\binom{n}{m} \equiv_p \binom{n_{d-1}}{m_{d-1}}\binom{n_{d-2}}{m_{d-2}}\cdots\binom{n_0}{m_0}$$

が成り立つ。（なお、$a < b$ のとき $\binom{a}{b} = 0$ であることを注意しておく。）

証明. $X := \binom{[0,n-1]}{m}$ と定める。二項係数の定義より $|X| = \binom{n}{m}$ である。

$\ell \in [0, d-1]$, $\alpha \in [0, n_\ell - 1]$ について

$$Y(\ell, \alpha) := \{(n_{d-1}\cdots n_{\ell+1}\alpha *_{\ell-1}\cdots *_1 *_0)_p \in \mathbb{Z}_{\ge 0} \mid i \in [0, \ell-1] \text{ のとき } *_i \in [0, p-1]\}$$

と定める。これらの集合たちは互いに交わらず、その和集合は $[0, n-1]$ と一致する。また、$k \in [0, d-2]$ と $x \in \mathbb{Z}_{\ge 0}$ に対して、x の p 進法表示 $x = (\cdots x_2x_1x_0)_p$ の k 桁目以下 x_k, …, x_1, x_0 をすべて $p-1$ に置き換えた数を $f_k(x)$ で表す。そして、$x \in Y(\ell, \alpha)$ について、$f_k(x) \le n-1$ のとき x の k 桁目 x_k を $x_k + 1 \bmod p$ に取り替えた値を $\sigma_k(x)$ で表し、$f_k(x) > n-1$ のとき $\sigma_k(x) := x$ とする。すると、$x \in Y(\ell, \alpha)$ について、$k \le \ell - 1$ のときは、$f_k(x) \le f_{\ell-1}(x) = (n_{d-1}\cdots n_{\ell+1}(\alpha+1)0\cdots 00)_p - 1 \le n-1$ を満たすので、

x は σ_k によって固定されない。さらに $Y(\ell,\alpha)$ の定義より $\sigma_k(x) \in Y(\ell,\alpha)$ である。一方、$k \geq \ell$ のときは、$f_k(x) \geq f_\ell(x) = (n_{d-1}\cdots n_{\ell+1}(p-1)\cdots(p-1)(p-1))_0 \geq n > n-1$ を満たすので、$\sigma_k(x) = x$ である。このことから集合 $Y(\ell,\alpha)$ はどの σ_k でも不変であり、$\sigma_\ell, \ldots, \sigma_{d-2}$ は $Y(\ell,\alpha)$ の元をすべて固定し、$\sigma_0, \ldots, \sigma_{\ell-1}$ は $Y(\ell,\alpha)$ のどの元も固定しない。これと $[0, n-1]$ が $Y(\ell,\alpha)$ たちに分割されることから、各 σ_k は $[0, n-1]$ からそれ自身への写像をなし、σ_k^p は $[0, n-1]$ 上の恒等写像となる。特に σ_k は全単射である。

$\ell_1 < \ell_2$ のとき σ_{ℓ_1} と σ_{ℓ_2} は可換である。実際、$x \in Y(\ell,\alpha)$ とすると、前段落の議論より、

- $\ell > \ell_2$ のとき、$\ell > \ell_1$ でもあるので、$(\sigma_{\ell_1} \circ \sigma_{\ell_2})(x)$ と $(\sigma_{\ell_2} \circ \sigma_{\ell_1})(x)$ は、どちらも x の ℓ_1 桁目と ℓ_2 桁目に（p を法として）1 ずつ加えたものであり、どちらの桁を先に変化させるかの違いしかない。よって $(\sigma_{\ell_1} \circ \sigma_{\ell_2})(x) = (\sigma_{\ell_2} \circ \sigma_{\ell_1})(x)$ が成り立つ。
- $\ell_2 \geq \ell > \ell_1$ のとき、σ_{ℓ_2} は $Y(\ell,\alpha)$ の元をすべて固定し、また $Y(\ell,\alpha)$ は σ_{ℓ_1} の作用で不変である。よって $(\sigma_{\ell_1} \circ \sigma_{\ell_2})(x) = \sigma_{\ell_1}(x) = (\sigma_{\ell_2} \circ \sigma_{\ell_1})(x)$ が成り立つ。
- $\ell_1 \geq \ell$ のとき、$\ell_2 \geq \ell$ でもあるので、σ_{ℓ_1} と σ_{ℓ_2} はともに x を固定する。よって $(\sigma_{\ell_1} \circ \sigma_{\ell_2})(x) = x = (\sigma_{\ell_2} \circ \sigma_{\ell_1})(x)$ が成り立つ。

よってどの場合にも $(\sigma_{\ell_1} \circ \sigma_{\ell_2})(x) = (\sigma_{\ell_2} \circ \sigma_{\ell_1})(x)$ が成り立つので、$\sigma_{\ell_1} \circ \sigma_{\ell_2} = \sigma_{\ell_2} \circ \sigma_{\ell_1}$ である。これと前段落の議論より、$\sigma_0, \ldots, \sigma_{d-2}$ が（写像の合成に関して）生成する群を G で表すと G は可換群であり、写像 $(\mathbb{Z}/p\mathbb{Z})^{d-1} \to G$, $(e_0, e_1, \ldots, e_{d-2}) \mapsto \sigma_0^{e_0}\sigma_1^{e_1}\cdots\sigma_{d-2}^{e_{d-2}}$ は全射準同型である。よって準同型定理より、G の位数 $|G|$ は $|(\mathbb{Z}/p\mathbb{Z})^{d-1}| = p^{d-1}$ の約数であり、p は素数であるから $|G|$ は p のべき乗の形である。

G の X への作用を $\tau \cdot \{x_1, \ldots, x_m\} := \{\tau(x_1), \ldots, \tau(x_m)\}$ で定める。この作用による X の軌道分解を考えると、各軌道の位数は G のある剰余群の位数と等しく、$|G|$ は素数 p のべき乗であるから、各軌道の位数も p のべき乗の形となる。よって、この作用による不動点の集合 $X_0 := \{S \in X \mid \tau \in G \text{ のとき } \tau \cdot S = S\}$ について、X_0 以外の X の点を含む軌道はどれも p の倍数の位数をもつので、$|X| \equiv_p |X_0|$ が成り立つ。あとは $|X_0|$ が主張の右辺と一致することを示せばよい。

$S \in X_0$ とする。$\ell \in [0, d-1]$, $\alpha \in [0, n_\ell - 1]$ について、$S \cap Y(\ell,\alpha) \neq \emptyset$ として、その要素の一つを x とする。上記の議論より $\sigma_0, \ldots, \sigma_{\ell-1}$ は $Y(\ell,\alpha)$ のどの元も固定しないので、それらの写像の定義より、x に G の元を施すことで $Y(\ell,\alpha)$ のすべての要素が得られる。そして $S \in X_0$ より、これらの要素はすべて S に属する。したがって、$S \cap Y(\ell,\alpha) = \emptyset$ または $Y(\ell,\alpha) \subseteq S$ が成り立つ。このことから、$I_\ell := \{\alpha \in [0, n_\ell - 1] \mid Y(\ell,\alpha) \subseteq S\}$ とおくと、$S = \bigcup_{\ell=0}^{d-1} \bigcup_{\alpha \in I_\ell} Y(\ell,\alpha)$ となる。逆に、上記の議論より各 $Y(\ell,\alpha)$ は G のどの元でも不変であるから、このような形の $S \in X$ は X_0 に属する。よって X_0 の元は、集合 I_ℓ たちの選び方によって定まる。ここで $c_\ell := |I_\ell|$ とすると、$|Y(\ell,\alpha)| = p^\ell$ より、対応する $S \in X_0$ について $|S| = \sum_{\ell=0}^{d-1} c_\ell p^\ell = (c_{d-1}\cdots c_1 c_0)_p$ が成り立つ。これが $|S| = m$ を満たすことは、すべての ℓ について $c_\ell = m_\ell$ を満たすことと同値である。よって $|X_0|$ は、各 ℓ について要素数 n_ℓ の集合 $[0, n_\ell - 1]$ から I_ℓ の m_ℓ 個の要素を選ぶ場合の数と等しい。後者は主張の右辺 $\binom{n_{d-1}}{m_{d-1}} \cdots \binom{n_1}{m_1}\binom{n_0}{m_0}$ に一致するので、主張が成り立つ。 □

参考文献

[1] E. Lucas, “Théorie des Fonctions Numériques Simplement Périodiques”, Amer. J. Math. **1**(3) (1878) 197–240