代数序論（第５回・2012/05/17）

演習問題の解答

[**2**] (p.11)

(i) $S_2 = \{(1), a\}$, $a = (1\ 2)$,
(ii) $S_3 = \{(1), a, b, c, d, e\}$, $a = (1\ 2\ 3)$, $b = (1\ 3\ 2)$, $c = (1\ 2)$, $d = (1\ 3)$, $e = (2\ 3)$,
(iii) $X_3 = \{(1), a, b\}$, $a = (1\ 2\ 3)$, $b = (1\ 3\ 2)$,
(iv) $X_4 = \{(1), a, b\}$, $a = (1\ 4\ 3)$, $b = (1\ 3\ 4)$,
(v) $X_5 = \{(1), a, b, c\}$, $a = (1\ 2\ 3\ 4)$, $b = (1\ 3)(2\ 4)$, $c = (1\ 4\ 3\ 2)$,
(vi) $X_6 = \{(1), a, b, c\}$, $a = (1\ 2)(3\ 4)$, $b = (1\ 3)(2\ 4)$, $c = (1\ 4)(2\ 3)$,
(vii) $X_7 = \{(1), a, b, c\}$, $a = (1\ 5\ 2\ 3)$, $b = (1\ 2)(5\ 3)$, $c = (1\ 3\ 2\ 5)$,
(viii) $X_8 = \{(1), a, b, c\}$, $a = (1\ 2)$, $b = (3\ 4)$, $c = (1\ 2)(3\ 4)$,
(ix) $X_9 = \{(1), a, b, c, d\}$, $a = (1\ 2\ 3\ 4\ 5)$, $b = (1\ 3\ 5\ 2\ 4)$, $c = (1\ 4\ 2\ 5\ 3)$, $d = (1\ 5\ 4\ 3\ 2)$.

(i) S_2

$\circ$	(1)	a
(1)	(1)	a
a	a	(1)

(ii) S_3

$\circ$	(1)	a	b	c	d	e
(1)	(1)	a	b	c	d	e
a	a	b	(1)	d	e	c
b	b	(1)	a	e	c	d
c	c	e	d	(1)	b	a
d	d	c	e	a	(1)	b
e	e	d	c	b	a	(1)

(iii) X_3, (iv) X_4

$\circ$	(1)	a	b
(1)	(1)	a	b
a	a	b	(1)
b	b	(1)	a

(v) X_5, (vii) X_7

$\circ$	(1)	a	b	c
(1)	(1)	a	b	c
a	a	b	c	(1)
b	b	c	(1)	a
c	c	(1)	a	b

(vi) X_6, (viii) X_8

$\circ$	(1)	a	b	c
(1)	(1)	a	b	c
a	a	(1)	c	b
b	b	c	(1)	a
c	c	b	a	(1)

(ix) X_9

$\circ$	(1)	a	b	c	d
(1)	(1)	a	b	c	d
a	a	b	c	d	(1)
b	b	c	d	(1)	a
c	c	d	(1)	a	b
d	d	(1)	a	b	c

[**3**] (p.11)

(i) $Y_1 = \{1, a\}$, $a = -1$,
(ii) $Y_2 = \{1, a, b\}$, $a = (-1 + \sqrt{-3})/2$, $b = (-1 - \sqrt{-3})/2$,
(iii) $Y_3 = \{1, a, b, c\}$, $a = \sqrt{-1}$, $b = -1$, $c = -\sqrt{-1}$.

(i) Y_1

$\cdot$	1	a
1	1	a
a	a	1

(ii) Y_2

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

(iii) Y_3

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

定義 (階乗)． 0 以上の整数 $n \in \mathbb{N} \cup \{0\}$ に対して，n の**階乗** (factorial) $n!$ を

$$\begin{cases} 0! := 1, \\ n! := n(n-1)\cdots 2 \cdot 1, \quad (n \in \mathbb{N}) \end{cases}$$

と定義する．

定義 (二項係数)． $n \in \mathbb{N} \cup \{0\}$ と $0 \leq k \leq n$ に対して，

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!}$$

を**二項係数** (binomial coefficient) とよぶ．

命題． $n \in \mathbb{N}$ と $1 \leq k \leq n$ に対して，以下が成り立つ：

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

定理 (二項定理)． $n \in \mathbb{N}$ に対して，以下が成り立つ：

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

定義 (フィボナッチ数列)． $F_1 = 1,\ F_2 = 1,\ F_n = F_{n-1} + F_{n-2},\ (n \geq 3)$ で定まる数列 $\{F_n\}_{n\in\mathbb{N}}$ を**フィボナッチ (Fibonacci) 数列**という．各項 F_n は n 番目の**フィボナッチ数**といわれる．

例． $\{F_n\}_{n\in\mathbb{N}}$ の最初の 20 項を書いてみる：

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$$

さらに 20 項ごとに求めてみると，読めないような数 (!) になってしまう：

$$\begin{aligned}
F_{20} &= 6765, \\
F_{40} &= 102334155, \\
F_{60} &= 1548008755920, \\
F_{80} &= 23416728348467685, \\
F_{100} &= 354224848179261915075, \\
F_{120} &= 5358359254990966640871840, \\
F_{140} &= 81055900096023504197206408605, \\
F_{160} &= 1226132595394188293000174702095995, \\
F_{180} &= 18547707689471986212190138521399707760, \\
F_{200} &= 280571172992510140037611932413038677189525.
\end{aligned}$$

例． n 項目 F_n が 1 つ前の $n-1$ 項目 F_{n-1} の何倍になっているかを計算してみる：

$$\begin{aligned}
F_2/F_1 &= 1.00000000, & F_7/F_6 &= 1.62500000, & F_{12}/F_{11} &= 1.61797753, & F_{17}/F_{16} &= 1.61803445, \\
F_3/F_2 &= 2.00000000, & F_8/F_7 &= 1.61538462, & F_{13}/F_{12} &= 1.61805556, & F_{18}/F_{17} &= 1.61803381, \\
F_4/F_3 &= 1.50000000, & F_9/F_8 &= 1.61904762, & F_{14}/F_{13} &= 1.61802575, & F_{19}/F_{18} &= 1.61803406, \\
F_5/F_4 &= 1.66666667, & F_{10}/F_9 &= 1.61764706, & F_{15}/F_{14} &= 1.61803714, & F_{20}/F_{19} &= 1.61803396, \\
F_6/F_5 &= 1.60000000, & F_{11}/F_{10} &= 1.61818182, & F_{16}/F_{15} &= 1.61803279, & F_{21}/F_{20} &= 1.61803400.
\end{aligned}$$

定義 (黄金比). $x^2 = x + 1$ を満たす実数は

$$\alpha := \frac{1+\sqrt{5}}{2}, \qquad \beta := \frac{1-\sqrt{5}}{2}$$

であり，特に，比 $1 : \alpha = 1.61803399\cdots$ は**黄金比** (golden ratio) と呼ばれている．

定理 (ビネの公式). フィボナッチ数列 $\{F_n\}_{n\in\mathbb{N}}$ の第 n 項は以下で与えられる：

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{1}{\sqrt{5}}\Big\{\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big\}.$$

定理 (フィボナッチ数の比の収束). フィボナッチ数列 $\{F_n\}_{n\in\mathbb{N}}$ に対して，

$$\lim_{n\to\infty}\frac{F_{n+1}}{F_n} = \alpha = \frac{1+\sqrt{5}}{2}.$$

法 (modulo) m の世界

定義 (法 m に関して合同). 整数 $a, b \in \mathbb{Z}$ が法 m に関して合同 (congruent) であるとは，$a - b$ が m で割り切れることと定義し，$a \equiv b \pmod{m}$ とかく．

m を法としたフィボナッチ数列.

$$\begin{aligned}
\{F_n \ (\mathrm{mod}\ 2)\}_{n\in\mathbb{N}} &: \mathbf{1}, \mathbf{1}, \mathbf{0}, 1, 1, 0, 1, 1, 0, 1, 1, 0, \ldots \\
\{F_n \ (\mathrm{mod}\ 3)\}_{n\in\mathbb{N}} &: \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{0}, \mathbf{2}, \mathbf{2}, \mathbf{1}, \mathbf{0}, 1, 1, 2, 0, 2, 2, 1, 0, \ldots \\
\{F_n \ (\mathrm{mod}\ 4)\}_{n\in\mathbb{N}} &: \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{1}, \mathbf{0}, 1, 1, 2, 3, 1, 0, 1, 1, 2, 3, 1, 0, \ldots \\
\{F_n \ (\mathrm{mod}\ 5)\}_{n\in\mathbb{N}} &: \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{0}, \mathbf{3}, \mathbf{3}, \mathbf{1}, \mathbf{4}, \mathbf{0}, \mathbf{4}, \mathbf{4}, \mathbf{3}, \mathbf{2}, \mathbf{0}, \mathbf{2}, \mathbf{2}, \mathbf{4}, \mathbf{1}, \mathbf{0}, 1, 1, 2, \ldots \\
\{F_n \ (\mathrm{mod}\ 6)\}_{n\in\mathbb{N}} &: \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{2}, \mathbf{1}, \mathbf{3}, \mathbf{4}, \mathbf{1}, \mathbf{5}, \mathbf{0}, \mathbf{5}, \mathbf{5}, \mathbf{4}, \mathbf{3}, \mathbf{1}, \mathbf{4}, \mathbf{5}, \mathbf{3}, \mathbf{2}, \mathbf{5}, \mathbf{1}, \mathbf{0}, 1, 1, 2, 3, \ldots
\end{aligned}$$

定理 (フィボナッチ数列の周期性). m を法としたフィボナッチ数列 $\{F_n \ (\mathrm{mod}\ m)\}_{n\in\mathbb{N}}$ は周期性をもつ．すなわち，ある自然数 $N \in \mathbb{N}$ が存在して，以下が成り立つ：

$$F_{n+N} \equiv F_n \pmod{m}, \quad n = 1, 2, \ldots$$

フィボナッチ数列の周期性の証明には，次の鳩の巣原理が有効に働く：

鳩の巣原理 (Pigeonhole principle), **Dirichlet**(ドイツ, 1805–1859) **の部屋割り論法.**
鳩の巣原理とは『整数 $n > m$ に対して，n 羽の鳩が m 個の巣に入っているとすると，ある巣には2羽以上の鳩が入っている』という原理のことを指す.

m を法としたパスカルの三角形.

$$\begin{array}{cccc}
m=2 & m=3 & m=4 & m=5 \\[6pt]
1 & 1 & 1 & 1 \\
1\ 1 & 1\ 1 & 1\ 1 & 1\ 1 \\
1\ 0\ 1 & 1\ 2\ 1 & 1\ 2\ 1 & 1\ 2\ 1 \\
1\ 1\ 1\ 1 & 1\ 0\ 0\ 1 & 1\ 3\ 3\ 1 & 1\ 3\ 3\ 1 \\
1\ 0\ 0\ 0\ 1 & 1\ 1\ 0\ 1\ 1 & 1\ 0\ 2\ 0\ 1 & 1\ 4\ 1\ 4\ 1 \\
1\ 1\ 0\ 0\ 1\ 1 & 1\ 2\ 1\ 1\ 2\ 1 & 1\ 1\ 2\ 2\ 1\ 1 & 1\ 0\ 0\ 0\ 0\ 1 \\
1\ 0\ 1\ 0\ 1\ 0\ 1 & 1\ 0\ 0\ 2\ 0\ 0\ 1 & 1\ 2\ 3\ 0\ 3\ 2\ 1 & 1\ 1\ 0\ 0\ 0\ 1\ 1 \\
1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 & 1\ 1\ 0\ 2\ 2\ 0\ 1\ 1 & 1\ 3\ 1\ 3\ 3\ 1\ 3\ 1 & 1\ 2\ 1\ 0\ 0\ 1\ 2\ 1
\end{array}$$

次の定理は，整数論の研究室に所属すれば証明を学ぶことができる (証明には，リーマンのゼータ関数を拡張したディリクレの L 関数というものが活躍する)：

Dirichlet の算術級数中の素数定理． $m \in \mathbb{N}$ と $a \in \mathbb{N}$ は互いに素とする．このとき，$mn + a$ 型の素数は無限に存在する．

Dirichlet の算術級数中の素数定理 (II)． $m \in \mathbb{N}$ と $a \in \mathbb{N}$ は互いに素とする．このとき，

$$\lim_{x\to\infty} \frac{\#\{x \text{ 以下の } mn+a \text{ 型の素数}\}}{\#\{x \text{ 以下の素数}\}} = \frac{1}{\#\{k \in \mathbb{N} \mid 1 \le k \le m \text{ かつ } k \text{ は } m \text{ と互いに素}\}}.$$

$m = 4$ の具体例 ($4n + 1$ 型の素数と $4n + 3$ 型の素数)．

200 以下の奇素数を $4n + 1$ 型と $4n + 3$ 型に分けてみる：
$\{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197\}$,
$\{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199\}$.

$$\#\{x \text{ 以下の } 4n+1 \text{ 型の素数}\} \le \#\{x \text{ 以下の } 4n+3 \text{ 型の素数}\}$$

かと思ってしまうが，さらに素数 26861 まで続けると初めて逆転現象が起こる (!):

x	5	17	41	100	200	461	$\cdots$	26849	26861	$\cdots$
$\#\{x$ 以下の $4n+1$ 型の素数$\}$	1	3	6	11	21	44	$\cdots$	1472	1473	$\cdots$
$\#\{x$ 以下の $4n+3$ 型の素数$\}$	1	3	6	13	24	44	$\cdots$	1472	1472	$\cdots$

それどころか，上述の Dirichlet の定理 (II) は次を主張している：

$$\lim_{x\to\infty} \frac{\#\{x \text{ 以下の } 4n+1 \text{ 型の素数}\}}{\#\{x \text{ 以下の素数}\}} = \lim_{x\to\infty} \frac{\#\{x \text{ 以下の } 4n+3 \text{ 型の素数}\}}{\#\{x \text{ 以下の素数}\}} = \frac{1}{2}.$$

定理 (リュカ, 1876)． $\{F_n\}_{n\in\mathbb{N}}$ をフィボナッチ数列，$[x]$ を $x \in \mathbb{R}$ のガウス記号とする．

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots + \binom{[n/2]}{[(n-1)/2]}.$$

演習問題 (小テスト・中間テストの予想問題)

[1] m を法としたパスカルの三角形を，蛍光ペンで色分けして作ってみよう！ ($m = 2, 3, 4, 5$)

[2] 次を示せ： (i) $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n$, (ii) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

[3] 10 段の階段を 1 段または 2 段ずつ昇る方法は何通りあるか？ 20 段ではどうか？

参考文献

[1] はじめての数論―発見と証明の大航海 ピタゴラスの定理から楕円曲線まで, ジョセフ・H. シルヴァーマン (著), 鈴木 治郎 (翻訳), ピアソンエデュケーション (2001).

[2] A Friendly Introduction To Number Theory (洋書), Joseph H. Silverman (著), Prentice Hall College Div; 3 版 (2005).

[3] フィボナッチ数の小宇宙―フィボナッチ数、リュカ数、黄金分割, 中村 滋 (著), 日本評論社; 改訂版版 (2008).