Number Theory

No.
Date: / /

- $\begin{cases} a \in \mathbb{Z} \\ b \in \mathbb{N} \end{cases}$, $\frac{a}{b} = \lfloor \frac{a}{b} \rfloor + \alpha$, $(0 \le \alpha < 1) \Rightarrow a = b\lfloor \frac{a}{b} \rfloor + b\alpha$
  $= bq + r$, $(0 \le r < b)$
- $a = bq$, $b \mid a$ $(b \ne 0)$
- 定理 (1) $a \mid b$, $b \mid a \Rightarrow a = \pm b$
  (2) $a \mid b$, $b \mid c \Rightarrow a \mid c$
  (3) $\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow$ (i) $kd \mid ka$ (iii) $d \mid ax+by$
  (ii) $d \mid a \pm b$
- 定義 (module) $\mathfrak{M} \subset \mathbb{Z}$, $\forall\, {a \atop b} \in \mathfrak{M} \Rightarrow a \pm b \in \mathfrak{M}$ $(a \in \mathfrak{M} \Rightarrow \langle a \rangle \subset \mathfrak{M})$
- 定理 $\mathfrak{M}$: module $\Rightarrow \mathfrak{M} = \langle d \rangle$, 證 (i) $\mathfrak{M} = \{0\}$ 或
  (ii) $d = \min\limits_{a \in \mathfrak{M},\, a>0} a$, $\forall n \in \mathfrak{M}$, $n = dq + r \Rightarrow r = 0$ $\quad 0 \le r < d$
- 例 (1) $\langle a \rangle = a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$
  (2) $\langle a, b \rangle = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\} = \langle d \rangle$
  (3) $\langle a_1, \dots, a_k \rangle = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \{a_1x_1 + \dots + a_kx_k \mid x_i \in \mathbb{Z}\}$
  (最大公約數)
- 定理 (1) $\exists\, x, y$, $d = ax + by$
  (2) $d \mid a$, $d \mid b$ $\quad \therefore d = (a, b)$
  (3) $e \mid a$, $e \mid b \Rightarrow e \mid d$
- 定理 $ax + by = n$ 有整數解 $\Leftrightarrow (a,b) \mid n$

質數, 互質 $(a \perp b)$

- 定理 (Euclid) ∞ 個 primes
- 定理 $a^m - 1$ prime $\Rightarrow \begin{cases} a = 2 \\ m: \text{prime} \end{cases}$ (Mersenne)
- 定理 $2^m + 1$ 〃 $\Rightarrow m = 2^k$ (Fermat)
- 定理 (Prime th) $\pi(x) \overset{\text{def}}{=} (\#\text{ primes} \le x) \approx \frac{x}{\ln x}$
  (i) $\lim\limits_{x \to \infty} \pi(x) = \infty$
  (ii) $\lim\limits_{x \to \infty} \frac{\pi(x)}{x} = 0$
  (iii) n^{th} prime $P_n \approx n \ln n$

- Euclid algorithm $(a, b) = (b, r)$, $a = bq + r$

$a = 323$, $b = 221$
$323 = 1 \cdot 221 + 102$
$221 = 2 \cdot 102 + 17$
$102 = 6 \cdot 17$

1	323	221	2
	221	204	
6	102	17	
	102		
	0		

$\Rightarrow 17 = b - 2 \cdot 102$
$= b - 2(a - b)$
$= -2a + 3b$

- $(323, 221)$
  $= (221, 102)$
  $= (102, 17) = 17$
- $(-2) \cdot 323 + 3 \cdot 221 = 17$

- 解 $323x + 221y = 85$ $\quad 85 = 17 \cdot 5$
  (甲) $323(-10) + 221 \cdot 15 = 85$ (特別解)
  (乙) $19x + 13y = 5$ $\quad (19, 13) = 1$
  $19(-2) + 13 \cdot 3 = 1$
  $19(\underset{+13t}{-10}) + 13(\underset{-19t}{15}) = 5$ (一般解)

- 定理 (1) $d \mid ab$, $(d, a) = 1 \Rightarrow d \mid b$
  (2) prime $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$

定理 (算數基本定理) $n = p_1^{k_1} \cdots p_r^{k_r}$ (唯一分解)

證: (1) $dx + ay = 1 \Rightarrow dbx + aby = b$

同餘 (Congruence)

- $a \equiv b \pmod{m} \iff m \mid a-b$

- **定理** (1) $a \equiv a \pmod{m}$
  (2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
  (3) $\left\{\begin{array}{l} a \equiv b \\ b \equiv c \end{array}\right. \pmod{m} \Rightarrow a \equiv c \pmod{m}$

  Equivalence class $= \{[0],[1],\dots,[m-1]\} = \mathbb{Z}_m$
  $[a] = \{k \equiv a \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$

- **定理** (1) $\left\{\begin{array}{l} a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array}\right. \Rightarrow \left\{\begin{array}{l} a \pm b \equiv c \pm d \\ ka \equiv kc \\ ab \equiv cd \end{array}\right. \pmod{m}$

  證 (1) $\left\{\begin{array}{l} m \mid a-c \\ m \mid b-d \end{array}\right. \Rightarrow m \mid (a \pm b)-(c \pm d)$
  $ab \equiv cb \equiv cd \pmod{m}$

  (2) $\left\{\begin{array}{l} \text{(i) } ka \equiv kb \pmod{m},\ k \perp m \Rightarrow a \equiv b \pmod{m} \\ \text{(ii) } ka \equiv kb \pmod{m}\ \left\{\begin{array}{l} k = k_0 d \\ m = m_0 d \end{array}\right. \Rightarrow a \equiv b \pmod{m_0} \end{array}\right.$
  $k_0 \perp m_0$

  (2) $m \mid k(a-b)$
  $m_0 d \mid k_0 d\,(a-b)$

  例 $\left\{\begin{array}{l} 13 \cdot 5 \equiv 7 \cdot 5 \pmod{6} \Rightarrow 13 \equiv 7 \pmod{6} \\ 5 \cdot 10 \equiv 14 \cdot 10 \pmod{6} \Rightarrow 5 \equiv 14 \pmod{3} \end{array}\right.$

  (Euler) $\varphi(m) := \#\, a,\ \begin{array}{l} 1 \le a < m \\ a \perp m \end{array}$

- **定理** $\left\{\begin{array}{l} \mathbb{Z}_m = \{[0],[1],\dots,[m-1]\} \\ \mathbb{Z}_m^* = \{[a] \mid 0 \le a \le m-1,\ a \perp m\} \end{array}\right.$ $\quad \begin{array}{l} |\mathbb{Z}_m| = m \\ |\mathbb{Z}_m^*| = \varphi(m) \end{array}$

  (1) $(\mathbb{Z}_m, +, \cdot)$ 環, (2) $(\mathbb{Z}_m^*, \cdot)$ 乘法群, (3) $\mathbb{Z}_p$ 有限域

  $\left\{\begin{array}{l} \mathbb{Z}_{12} = \{[0],[1],[2],\dots,[10],[11]\} \\ \mathbb{Z}_{12}^* = \{[1],[5],[7],[11]\} \\ \mathbb{Z}_7 = \{[0],[1],\dots,[6]\} \end{array}\right.$

  $\left\{\begin{array}{l} [a] \pm [b] = [a \pm b] \\ [a] \cdot [b] = [a \cdot b] \end{array}\right.$, $\mathbb{Z}_{12}$: $\left\{\begin{array}{l} 9 \equiv 33 \\ 5 \equiv 17 \end{array}\right. \pmod{12}$ $\left\{\begin{array}{l} 9+5 \equiv 33+17 \equiv 2 \\ 9-5 \equiv 33-17 \equiv 4 \\ 9 \cdot 5 \equiv 33 \cdot 17 \equiv 9 \end{array}\right. \pmod{12}$

  $\left\{\begin{array}{l} [a] + [0] = [a] \\ [a] \cdot [1] = [a] \end{array}\right.$ $\quad [9]+[5] = [2],\ [9]-[5] = [4],\ [9][5] = [9]$

- **定義** $\{x_1, \dots, x_m\}$ ($x_i \not\equiv x_j \bmod m$), Complete residue system $(= \mathbb{Z}_m)$
  $\{x_1, \dots, x_{\varphi(m)}\}$ (〃 且 $x_i \perp m$), reduced 〃 〃 $(= \mathbb{Z}_m^*)$

- **定理** $a \perp m$ $\left\{\begin{array}{l} (1)\ \{x_1,\dots,x_m\} \text{ complete r.s.} \Rightarrow \{ax_1,\dots,ax_m\} \text{ also},\quad a\mathbb{Z}_m \equiv \mathbb{Z}_m \\ (2)\ \{x_1,\dots,x_{\varphi(m)}\} \text{ reduced 〃} \Rightarrow \{ax_1,\dots,ax_{\varphi(m)}\} \text{ 〃},\quad a\mathbb{Z}_m^* \equiv \mathbb{Z}_m^* \end{array}\right. \pmod{m}$

  證 (1) $ax_i \equiv ax_j \bmod m \Rightarrow m \mid a(x_i - x_j)$
  $\Rightarrow m \mid x_i - x_j$
  $\Rightarrow x_i \equiv x_j$

  (2) $ax_i \perp m$
  (1') $(a,m) = d,\ ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{m_0}$

例 $5\mathbb{Z}_{12} = \{0,5,10,15,20,25,30,35,40,45,50,55\}$, $\quad 5\mathbb{Z}_{12}^* = \{5,25,35,55\} \pmod{12}$
$\equiv \{0,5,10,3,8,1,6,11,4,9,2,7\}$ $\quad \equiv \{5,1,11,7\}$
$\pmod{12}$

$10\mathbb{Z}_{12} = \{0,10,20,30,40,50,60,70,80,90,100,110\}$
$(10,12) = 2 \quad \equiv \{0,10,8,6,4,2,0,10,8,6,4,2\} = 2 * \{0,5,4,3,2,1\}^2$

$\left(\begin{array}{l} 10a \equiv 10b \pmod{12} \\ \Rightarrow a \equiv b \pmod{6} \end{array}\right.$

• **定理** (Euler) $a\perp m,\quad a^{\varphi(m)}\equiv 1 \pmod m$ **証**: $x_1\cdots x_{\varphi(m)} \equiv a^{\varphi(m)}\, x_1\cdots x_{\varphi(m)} \pmod m$

• **定理** (Fermat) p: prime, $a^p\equiv a \pmod p$ $\begin{cases} \text{(i) } p\mid a, & a\equiv a^p\equiv 0 \pmod p \\ \text{(ii) } p\perp a, & a^{p-1}\equiv 1 \quad (\ 〃\ ) \end{cases}$

• **定理** (Wilson) p: prime $\Longleftrightarrow (p-1)! \overset{(p-1)}{\equiv} -1 \pmod p$ $p=11$

証 "$\Rightarrow$" $\forall\ 1\le k\le p-1$ $\begin{cases} k x_k \equiv 1 \pmod p \\ k k \equiv 1 \ (\ 〃\ ) \Rightarrow k=\pm 1 \end{cases}$ $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

"$\Leftarrow$" $\underset{(1\le d<p)}{d\mid p} \Rightarrow (p-1)! \equiv -1 \pmod d \Rightarrow 0\equiv -1 \pmod d \Rightarrow d=1$ #

• **定義** g: 積性函數 (multiplicative): $m\perp n \Rightarrow g(mn)=g(m)g(n) \Longleftrightarrow \begin{cases} g(p_1^{k_1}\cdots p_r^{k_r}) = g(p_1^{k_1})\cdots g(p_r^{k_r}) \\ g(1)=1 \end{cases}$

• (Euler-totient) $\varphi(n) := \#d,\ 1\le d\le n,\ d\perp n$

(1) φ: 積性

(2) p: prime, $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$

(3) $m=p_1^{k_1}\cdots p_r^{k_r}$, $\varphi(m) = m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$

(4) $\sum_{d\mid m}\varphi(d) = m$

(1)+(2) $\Longleftrightarrow$ (3)
(*) (*) (4) (甲)

(*): 定理2 + 推論, p5

証 (3) $m=2^3\cdot 3^2\cdot 5$, $\varphi(m) = m - \frac{m}{2} - \frac{m}{3} - \frac{m}{5} + \frac{m}{2\cdot 3} + \frac{m}{3\cdot 5} + \frac{m}{2\cdot 5} - \frac{m}{2\cdot 3\cdot 5}$

$= m\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$d\in (1+2+2^2+2^3)(1+3+3^2)(1+5)$

(4) 〃 (甲) $\sum_{d\mid m}\varphi(d) = \left(1+\varphi(2)+\varphi(2^2)+\varphi(2^3)\right)\left(1+\varphi(3)+\varphi(3^2)\right)\left(1+\varphi(5)\right)$

$= \left(1+(2-1)+(2^2-2)+(2^3-2^2)\right)\left(1+(3-1)+(3^2-3)\right)\left(1+(5-1)\right)$

$= 2^3\cdot 3^2\cdot 5$

(乙) $\left\{\frac{12}{12}, \frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}\right\}$ $m=12$

(約分) $\Rightarrow \left\{\frac{1}{1}, \left(\frac{1}{2}\right), \left(\frac{1}{3}, \frac{2}{3}\right), \left(\frac{1}{4}, \frac{3}{4}\right), \left(\frac{1}{6}, \frac{5}{6}\right), \left(\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}\right)\right\}$

$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12) = 12$

• (Möbius) $\mu(n) = \mu(p_1^{k_1}\cdots p_r^{k_r}) := \begin{cases} (-1)^r & k_1=k_2=\cdots=k_r=1 \\ 0 & \text{else} \end{cases}$ $(\mu(1)=1)$

(1) μ: 積性

(2) $\sum_{d\mid m}\mu(d) = \delta_{m=1}$

証: (1) $\mu(p_1^{k_1}\cdots p_r^{k_r}\cdot q_1^{h_1}\cdots q_s^{h_s}) = \mu(p_1^{k_1}\cdots p_r^{k_r})\,\mu(q_1^{h_1}\cdots q_s^{h_s})$

(2) $\sum_{d\mid m}\mu(d) = 1+\mu(2)+\mu(3)+\mu(5)+\mu(2\cdot 3)+\mu(3\cdot 5)+\mu(2\cdot 5)+\mu(2\cdot 3\cdot 5)$

$m=2^3\cdot 3^2\cdot 5$ $= 1+\binom{3}{1}(-1)+\binom{3}{2}(-1)^2+\binom{3}{3}(-1)^3 = (1-1)^3 = 0$

No.
Date: / /

- **定理** (Chinese remainder th) $m_i \perp m_j,\ \forall i \neq j$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$ 有唯一解 $\bmod (m_1 m_2 \cdots m_n)$

証
$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod 5 \\ x \equiv c \pmod 7 \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

(唯一)
$$\begin{cases} x \equiv a \equiv y \pmod 3 \\ x \equiv b \equiv y \pmod 5 \\ x \equiv c \equiv y \pmod 7 \end{cases} \Leftrightarrow \begin{cases} 3 \mid (x-y) \\ 5 \mid (x-y) \\ 7 \mid (x-y) \end{cases} \Leftrightarrow 3\cdot5\cdot7 \mid (x-y)$$

(存在)
$$x = a\cdot70 + b\cdot21 + c\cdot15 \pmod{105}$$
$$= 2\cdot70 + 3\cdot21 + 2\cdot15 \ (\ \ ''\ \ ) = 233 \pmod{105} = 23$$

$u\cdot5\cdot7 \equiv 1 \pmod 3$ $\quad w\cdot3\cdot5 \equiv 1 \pmod 7$ $\quad \left(\begin{array}{l} 35u \equiv 1 \pmod 3 \\ \Leftrightarrow 35u - 3k = 1 \end{array} \right)$

$v\cdot3\cdot7 \equiv 1 \pmod 5$ $\qquad u = 2$

(或)

$$70 \equiv \begin{cases} 1 \\ 0 \\ 0 \end{cases},\quad 21 \equiv \begin{cases} 0 \\ 1 \\ 0 \end{cases},\quad 15 \equiv \begin{cases} 0 & \pmod 3 \\ 0 & \pmod 5 \\ 1 & \pmod 7 \end{cases}$$

$$a\cdot70 + b\cdot21 + c\cdot15 \equiv \begin{cases} a+0+0 & \pmod 3 \\ 0+b+0 & \pmod 5 \\ 0+0+c & \pmod 7 \end{cases}$$

- **Residue number system**: $m \perp n$, $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ $\quad \left(\begin{array}{l} x = hm + a \\ \ \ = kn + b \end{array} \right)$

x mod 12	x mod 3	x mod 4
0	0	0
1	1	1
2	2	2
3	0	3
4	1	0
5	2	1
6	0	2
7	1	3
8	2	0
9	0	1
10	1	2
11	2	3

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, $\qquad \mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

$x = (a, b)$

$5 = (2, 1)$

$+)\ 11 = (2, 3)$

$4 \equiv 16 = (1, 0)$

$7 \equiv 55 = (1, 3)$

parallel

$x \perp mn \Leftrightarrow \begin{cases} a \perp m \\ b \perp n \end{cases}$

証: "$\Leftarrow$" $\begin{cases} p \mid x \\ p \mid mn \end{cases}$, $\ p \mid m \Rightarrow p \mid a$ (*)

"$\Rightarrow$"

$m \perp n \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$, $\quad \mathbb{Z}_{12}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_4^*$

Möbius Transformation

- **定義** (1) g 積性函數：$m \perp n$, $g(mn) = g(m)g(n)$ $\iff \begin{cases} g(1) = 1 \\ g(p_1^{k_1} \cdots p_r^{k_r}) = g(p_1^{k_1}) \cdots g(p_r^{k_r}) \end{cases}$

  (2) Möbius 函數 μ：$\sum_{d|m} \mu(d) = \delta_{m=1} = \begin{cases} 1 & m=1 \\ 0 & \text{else} \end{cases}$ (recursive 定義)

$\Downarrow$

m	1	2	3	4	5	6	7	8	9	10	11	12	15	30
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	1	-1

$m = p^k$, $0 = 1 + \mu(p) + \mu(p^2) + \cdots + \mu(p^k)$

$\mu(p) = -1$, $\mu(p^2) = \mu(p^3) = \cdots = 0$

- Möbius transf：$f \longrightarrow g(m) = \sum_{d|m} f(d)$

  $\mu \to \delta_{m=1}$

  $\varphi \to m$

  $1 \to \tau(m) = \#$因數, $= 4 \cdot 3 \cdot 2$

  $m \to \sigma(m) =$ 因數和, $= (1+2+2^2+2^3)(1+3+3^2)(1+5)$ $\quad m = 2^3 3^2 5$

(Möbius Inversion)

- **定理 1** $g(m) = \sum_{d|m} f(d) \iff f(m) = \sum_{d|m} \mu(d) g(\frac{m}{d})$ $\left[= \sum_{dk=m} \mu(d) g(k) = \sum_{d|m} \mu(\frac{m}{d}) g(d) \right]$

- **定理 2** f 積性 $\iff$ g 積性

- **推論**

  (1) $\delta_{m=1}$, m, 1 積性 $\Rightarrow \mu, \varphi, \tau, \sigma$ 積性

  (2) $\delta_{m=1} = \sum_{d|m} \mu(d) \Rightarrow \mu(m) = \begin{cases} (-1)^r & m = p_1 \cdots p_r \\ 0 & \text{else} \end{cases}$ $\quad \mu(m) = \mu(p_1^{k_1} \cdots p_r^{k_r}) = \mu(p_1^{k_1}) \cdots \mu(p_r^{k_r})$

  (3) $m = \sum_{d|m} \varphi(d) \Rightarrow \varphi(m) = \sum_{d|m} \mu(d) \frac{m}{d}$ $\quad (m = 2^3 3^2 5^4)$

  $= m\left[1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2}\frac{1}{3} + \frac{1}{2}\frac{1}{5} + \frac{1}{3}\frac{1}{5} - \frac{1}{2}\frac{1}{3}\frac{1}{5}\right]$

  $= m(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$ $= m(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})$

  (4) 環狀項鍊 $\begin{cases} m \text{ beads} \\ c \text{ colors} \end{cases}$ 個數 $N(m,c) = ?$ $\quad f(x+d) = f(x)$, period $= d$

  $N(d) = \#$ with period d

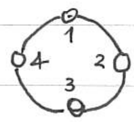
  - $c^m = \sum_{d|m} d N(d)$ (直線排列)
  - $m N(m) = \sum_{d|m} \mu(d) c^{\frac{m}{d}}$
  - $N(m,c) = \sum_{k|m} N(k)$

    $= \sum_{k|m} \frac{1}{k} \sum_{d|k} \mu(d) c^{\frac{k}{d}}$

    $\overset{?}{=} \frac{1}{m} \sum_{d|m} \varphi(d) c^{\frac{m}{d}}$
  - $N(4,2) = \frac{1}{4}\left[\varphi(1)2^4 + \varphi(2)2^2 + \varphi(4)2^1\right]$

    $= 6$

  例 $m = 4$, $C = 2$ $(0,1)$



  - $2^4 = 16$
  - $d = 1$, $N(1) = 2$ $\begin{cases} 0000 \\ 1111 \end{cases}$

    $d = 2$, $N(2) = 1$ $\{ 0101 \to 1010$

    $d = 4$, $N(4) = 3$ $\begin{cases} 0111 \to 1011, 1101, 1110 \\ 0011 \to 1001, 1100, 0110 \\ 0001 \to 1000, 0100, 0010 \end{cases}$
  - $2^4 = 1 \cdot N(1) + 2 \cdot N(2) + 4 \cdot N(4)$
  - $N(1) = \mu(1) 2^1 = 2$

    $N(2) = \frac{1}{2}\left[\mu(1)2^2 + \mu(2)2^1\right] = 1$

    $N(4) = \frac{1}{4}\left[\mu(1)2^4 + \mu(2)2^2 + \mu(4)2^1\right] = 3$
  - $N(4,2) = N(1) + N(2) + N(4) = 6$

定理証明

No.
Date: / /

- **定理1** $g(m)=\sum_{d|m} f(d) \iff f(m)=\sum_{d|m}\mu(d)\,g\left(\frac{m}{d}\right)$ $\quad\left(\sum_{d|m}\mu(d)=\delta_{m=1}\right)$

証 "⇒"

$$\begin{aligned}\sum_{d|m}\mu(d)\,g\left(\tfrac{m}{d}\right) &\overset{m=12}{=} \mu(1)g(12)+\mu(2)g(6)+\mu(3)g(4)+\mu(4)g(3)+\mu(6)g(2)+\mu(12)g(1)\\
&= \mu(1)\,[f(1)+f(2)+f(3)+f(4)+f(6)+f(12)]\\
&\quad+\mu(2)\,[f(1)+f(2)+f(3)+f(6)]\\
&\quad+\mu(3)\,[f(1)+f(2)+f(4)]\\
&\quad+\mu(4)\,[f(1)+f(3)]\\
&\quad+\mu(6)\,[f(1)+f(2)]\\
&\quad+\mu(12)\,[f(1)]\\
&= f(12)\end{aligned}$$

"⇐"

$$\begin{aligned}\sum_{d|m} f(d) &\overset{m=12}{=} f(1)+f(2)+f(3)+f(4)+f(6)+f(12)\\
&= [\mu(1)g(1)]\\
&\quad+[\mu(1)g(2)+\mu(2)g(1)]\\
&\quad+[\mu(1)g(3)+\mu(3)g(1)]\\
&\quad+[\mu(1)g(4)+\mu(2)g(2)+\mu(4)g(1)]\\
&\quad+[\mu(1)g(6)+\mu(2)g(3)+\mu(3)g(2)+\mu(6)g(1)]\\
&\quad+[\mu(1)g(12)+\mu(2)g(6)+\mu(3)g(4)+\mu(4)g(3)+\mu(6)g(2)+\mu(12)g(1)]\\
&= g(12)\end{aligned}$$

- **定理2** f: 積性 $\iff$ g 積性 $\quad\left\{\begin{array}{l}\forall\, ab<n,\ a\perp b\\ f(ab)=f(a)f(b)\end{array}\right.$

証 "⇐" 已知 g 積性, 擬証 f 積性 for n $(=12)$ by induction:

$g(2^2\cdot 3)=g(2^2)\,g(3) \overset{?}{\Longrightarrow} f(2^2\cdot 3)=f(2^2)\,f(3)$

$$g(2^2\cdot 3)=\sum_{d|12} f(d)=\sum_{\substack{a|2^2\\ b|3}} f(ab)=f(1\cdot 1)+f(1\cdot 3)+f(2\cdot 1)+f(2\cdot 3)+f(2^2\cdot 1)+\underline{f(2^2\cdot 3)}$$

$$\begin{aligned}g(2^2)\,g(3) &= \Big(\sum_{a|2^2} f(a)\Big)\Big(\sum_{b|3} f(b)\Big) = [f(1)+f(2)+f(2^2)]\,[f(1)+f(3)]\\
&= f(1)f(1)+f(1)f(3)+f(2)f(1)+f(2)f(3)\\
&\quad+f(2^2)f(1)+\underline{f(2^2)f(3)}\end{aligned}$$

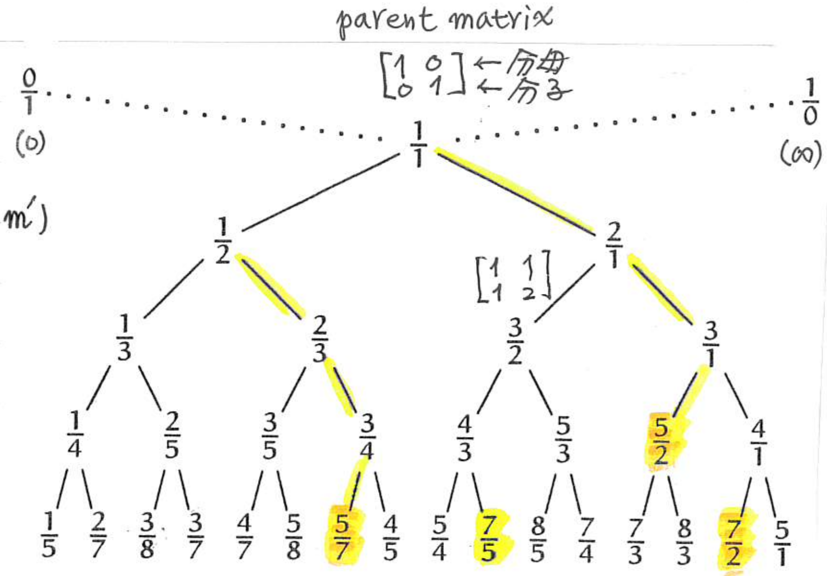
$\Rightarrow f(2^2\cdot 3)=f(2^2)\,f(3)$

"⇒"

$$\left(\begin{array}{l} d\,|\,2^2\cdot 3:\ (1+2+2^2)\cdot(1+3)\\ d=\qquad a\qquad\cdot\quad b\end{array}\right)$$

Stern-Brocot tree : Binary search tree for reduced fractions (最約分數)

(1) 左右反对稱



(2) Binary search tree:

$$\frac{m}{n} < \frac{m+m'}{n+n'} < \frac{m'}{n'} \qquad (mn' < nm')$$

(3) $\begin{vmatrix} n & n' \\ m & m' \end{vmatrix} = 1$

$$\Rightarrow \begin{vmatrix} n & n+n' \\ m & m+m' \end{vmatrix} = \begin{vmatrix} n+n' & n' \\ m+m' & m' \end{vmatrix} = 1$$

(4) $n \perp m$

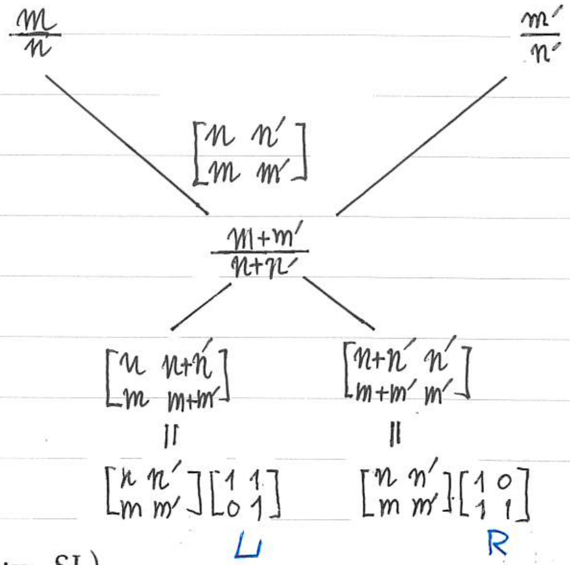
(5) $\frac{m}{n} \in \mathbb{Q}^+$, 恰一次 (i) 唯一 (∵(2)) (ii) 存在.

(6) $\mathbb{Q}^+ \longleftrightarrow \{L, R\}^*$ (number system)

"←" $LRRL = \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix}^2\begin{bmatrix}1&1\\0&1\end{bmatrix} = \begin{bmatrix}3&4\\2&3\end{bmatrix}$

$f: \begin{bmatrix}3&4\\2&3\end{bmatrix} \longrightarrow \frac{5}{7}$

"→" $\frac{m}{n} \longrightarrow ?$

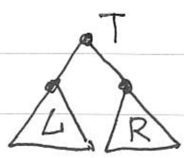


(甲) Binary search:

- S := I;
  while m/n ≠ f(S) **do**
  if m/n < f(S) **then** (output(L); S := SL)
  else (output(R); S := SR)

(乙) subtrees 相似性

- **while** m ≠ n **do**
  if m < n **then** (output(L); n := n − m)
  else (output(R); m := m − n)



- m/n = 5/7

- m = 5 5 3 1 1
  n = 7 2 2 2 1
  output L R R L

L ↔ T ↔ R

$\frac{m}{n+m}$ $\quad \frac{m}{n}$ $\quad \frac{n+m}{n}$

$RRL = \frac{5}{7} \quad \frac{5}{2} \quad \frac{7}{2}$