分数の小数展開の秘密

岩手県立一関第一高等学校理数科 2 年課題研究数学 B 班
永山虹空　鈴木智也　細川享平　徳永卓　佐々木拓海

2020 年 3 月 5 日

There is an amusing and amazing theorem on repeating decimals. It is called “Midy’s Theorem”. We formulate our own version, and investigate the secret of the theorem.
We found how to know the length of repeating decimals, if the fraction has the Midy’s property (999 rule) which was not mentioned by Midy, and prooved the Midy’s theorm by ourselves. Moreover, we have some extension of it.

[Keyword] repeating decimals, Midy’s Theorem

1　はじめに

1868 年, フランスの数学者である E.Midy は, 驚くべき数論を証明した. 以下がその定理である.
定理：p を 5 より大きい素数とし,m(m は正の整数) と p は互いに素とする.m/p の循環節の長さが偶数になる (2k とおく) とき, 循環節の初めの k 桁と最後の k 桁の合計は常に 999・・・9 となる.
例えば 3/7 は

$$3/7 = 0.\dot{4}28571\dot{}$$

となる.3/7 の循環節は [428571] だが, これを前半部と後半部に分けると [428]、[571] となり, これらを足すと [999] となる.
我々は 10 進数で 100 までの自然数の逆数を調べ,Midy の定理で性質が示された数と, そうでない数における循環節の長さについて様々な場合があることを発見した. この論文では, 分数の循環節の長さがどのように決定されるかを示し, 我々が学校で習う基本的な数論だけを使用し Midy の定理を証明している.

証明　proof1　鈴木智也　proof2　徳永卓
proof3　細川享平　proof4　永山虹空

2　商と余りの作る数列

$\frac{1}{n}$ の循環節が持つ性質を紐解くために, まず初めに $1 \div 7$ の筆算を表示する.

$$\begin{array}{r} 0.142857 \\ 7\,)\,10 \\ \underline{7} \\ 30 \\ \underline{28} \\ 20 \\ \underline{14} \\ 60 \\ \underline{56} \\ 40 \\ \underline{35} \\ 50 \\ \underline{49} \\ 1 \end{array} \quad \begin{array}{l} \\ \\ \Longleftarrow r_1 \\ \\ \Longleftarrow r_2 \\ \\ \Longleftarrow r_3 \\ \\ \Longleftarrow r_4 \\ \\ \Longleftarrow r_5 \\ \\ \Longleftarrow r_6 \end{array}$$

各段で行われている計算は, 次のようになる.

$$r_0 = 7 \times 0 + r_0, \quad q_0 = 0\,,\ r_0 = 1 \quad \cdots \quad (0)$$
$$r_0 \times 10 = 7 \times 1 + 3,\ q_1 = 1\,,\ r_1 = 3 \quad \cdots \quad (1)$$
$$r_1 \times 10 = 7 \times 4 + 2,\ q_2 = 4\,,\ r_2 = 2 \quad \cdots \quad (2)$$
$$r_2 \times 10 = 7 \times 2 + 3,\ q_3 = 2\,,\ r_3 = 6 \quad \cdots \quad (3)$$
$$r_3 \times 10 = 7 \times 8 + 4,\ q_4 = 8\,,\ r_4 = 4 \quad \cdots \quad (4)$$
$$r_4 \times 10 = 7 \times 5 + 5,\ q_5 = 5\,,\ r_5 = 5 \quad \cdots \quad (5)$$
$$r_5 \times 10 = 7 \times 7 + 1,\ q_6 = 7\,,\ r_6 = 1 \quad \cdots \quad (6)$$

$r_6 = r_0 = 1$ となっているので, この筆算のあとには (1)〜(6) 続く.
これらの筆算と式から商が作る数列は $1, 4, 2, 8, 5, 7$, 余りが作る数列は $1, 3, 2, 6, 4, 5$ であると言える.
また視点を変えて見てみると,

$$\begin{array}{r} 1 \\ 7\,)\,10 \\ \underline{7} \\ 3 \end{array} \quad \Longleftarrow \quad r_1 \qquad \begin{array}{r} 14 \\ 7\,)\,100 \\ \underline{7} \\ 30 \\ \underline{28} \\ 2 \end{array} \quad \Longleftarrow \quad r_2$$

$10 \div 7$　　$10^2 \div 7$

$$
\begin{array}{r}
\quad 1\ \ 4\ \ 2 \\
\hline
7\ )\ 1\ \ 0\ \ 0\ \ 0 \\
\quad\ 7 \\
\hline
\quad\ 3 \\
\quad\ 2\ \ 8 \\
\hline
\quad\ \ 2\ \ 0 \\
\quad\ \ 1\ \ 4 \\
\hline
\quad\ \ \ 6
\end{array}
\qquad \Longleftarrow \quad r_3 \qquad
\begin{array}{r}
\quad 1\ \ 4\ \ 2\ \ 8 \\
\hline
7\ )\ 1\ \ 0\ \ 0\ \ 0\ \ 0 \\
\quad\ 7 \\
\hline
\quad\ 3 \\
\quad\ 2\ \ 8 \\
\hline
\quad\ \ 2\ \ 0 \\
\quad\ \ 1\ \ 4 \\
\hline
\quad\ \ \ 6\ \ 0 \\
\quad\ \ \ 5\ \ 6 \\
\hline
\quad\ \ \ \ 4
\end{array}
$$

$10^3 \div 7$ $\qquad\qquad$ $10^4 \div 7$

上の４つの筆算から次のような性質が得られた.

Theorem 1. 一般に $1 \div n$ の筆算過程における余りがなす数列 $\{r_n\}$ は次の式で表される.

$$r_n \equiv 10^n \pmod{n}$$

10 進法小数表示だけでなく，あらゆる自然数 a における a 進法小数表示での $\dfrac{1}{n}$ の性質を調査するために，商がつくる数列 $\{q_n\}$ と余りが作る数列 $\{r_n\}$ を調査した.

商がつくる数列 $\{q_n\}$ と余りが作る数列 $\{r_n\}$ は，次のように決定される.

q_0 と r_0 は, $\qquad 1 = q_0 \times n + r_0 \qquad (0)$

よって $\ q_0 = 0,\ r_0 = 1$

$(0)\times a$ より $\quad a = aq_0 \times n + ar_0 \qquad (※)$

次に, $q_1,\ r_1$ を求める．これらは $a \cdot r_0 \div n$ の商と余りにより決定される.

$$
\begin{aligned}
ar_0 &= q_1 \times n + r_1 \\
&= q_0 \times n + ar_0 = aq_0 \times n + q_1 \times n + r_1 \\
&= (aq_0 + q_1) \times n + r_1 \qquad (1)
\end{aligned}
$$

$(1)\times a$ より，$a^2 = a\,(aq_0 + q_1) \times n + ar_1 \qquad (※)$

$r_1, r_2,\ \cdots r_k$ と $q_1, q_2,\ \cdots q_k$ が決定されるとき,

$$a^k r_0 = \left(a^k q_0 + a^{k-1} q_1 + \cdots + aq_{k-1} + q_k\right) \times n + r_k \qquad (k)$$

が成り立ち，$(k)\times a$ よりが,

$$
\begin{aligned}
&a \times a^k r_0 \\
&= a\left(a^k q_0 + a^{k-1} q_1 + \cdots + aq_{k-1} + q_k\right) \times n + ar_k \qquad (☆)
\end{aligned}
$$

$q_{k+1},\ r_{k+1}$ は $a \cdot r_k \div n$, and $ar_k = q_{k+1} \times n + r_{k+1}$ の商と余りの数列であるから次のような計算が成り立つ.

$$a^{k+1} r_0 = a\left(a^{k+1} q_0 + a^k q_1 + \cdots + aq_k + q_{k+1}\right) \times n + r_{k+1} \qquad (k+1)$$

したがって，$1 \div n$ の商と余りの数列 $\{q_n\}$ と $\{r_n\}$ は誘導的に決定される.

$$r_n \equiv a^n \times r_0 \pmod{n}$$

また，$r_0 = 1$ より

$$r_n \equiv a^n \pmod{n}$$

Theorem 2. a 進数での $\dfrac{1}{n}$ の計算過程で現れる余りの数列 $\{r_k\}$ は次のようになる.

$$r_k \equiv a^k \qquad (\bmod\ n)$$

(※),(☆),$(k+1)$ より，我々は次の結論を得た.

Corollary 1. $\dfrac{1}{n}$ の a 進小数展開を計算していくときに現れる余りの系列 $r_1, r_2, r_3,\ \cdots$ は

$$r_k \equiv r_1^k \qquad (\bmod\ n)$$

ただし，$r_1 = \mathrm{Mod}\,(a, n)$

が成り立つ.

ただし，a を n で割った余りを $\mathrm{Mod}\,(a, n)$ と表した.

. 式 $(k+1)$ と式 (☆) よ Proof り，$r_{k+1} \equiv a \cdot r_k$

さらに式 (※) $a = aq_0 \times n + ar_0$ より

$$r_{k+1} \equiv a \cdot r_k = (aq_0 \times n + ar_0) \cdot r_k \equiv ar_0 \cdot r_k \equiv r_1 \cdot r_k$$

が成り立つ.

したがって，数列 $\{r_k\}$ は初項が r_1, 公比が r_1 の等比数列になるので

$$r_k \equiv r_1^k \qquad (\bmod\ n)$$

が成り立つ.

3　循環しない分数

たとえば, $\dfrac{1}{2} = 0.5,\ \dfrac{1}{4} = 0.25,\ \dfrac{1}{5} = 0.2$ のように，無限小数にはならない分数もある．$1 \geqq n \geqq 100$ の範囲において, $\dfrac{1}{n}$ の小数展開が循環しない n をあげると

1, 2, 4, 5, 8, 20, 25, 32, 40, 50, 80, 100

である．このことから次のことがわかる.

Proposition 1.　自然数 n が

$n = 2^k \cdot 5^l \quad (\ k = 0, 1, 2,\ \cdots,\ l = 0, 1, 2,\ \cdots\ )$

であるとき, $\dfrac{1}{n}$ は有限小数となる.

逆に, $\dfrac{1}{n}$ が有限小数となるとすると，n は上記のように表すことができる.

Proof 1.

(1) $k \geqq l$ のとき

$$\frac{1}{n} = \frac{1}{2^k \cdot 5^l} = \frac{5^{k-l}}{2^k \cdot 5^k} = \frac{5^{k-l}}{10^k}$$

ここで，5^{k-l} を 10 進法表記したものを右詰にして左に 0 を補って $k-1$ 桁の数の列を作ったものを $[5^{k-l}]$ と表すこととすれば

$$\frac{1}{n}=0.\underbrace{[5^{k-l}]}_{k\text{ 桁}}$$

となり，有限小数となる．

(2) $k<l$ のときは

$$\frac{1}{n}=\frac{1}{2^k\cdot 5^l}=\frac{2^{l-k}}{2^l\cdot 5^l}=\frac{2^{l-k}}{10^l}$$

ここで，2^{l-k} を 10 進法表記したものを右詰にして左に 0 を補って $l-1$ 桁の数の列を作ったものを $[2^{l-k}]$ と表すこととすれば

$$\frac{1}{n}=0.\underbrace{[2^{l-k}]}_{l\text{ 桁}}$$

となり，有限小数となる．

逆に，$\dfrac{1}{n}$ が有限小数 $0.a_1a_2\ \cdots a_m$ で表されるとすると

$$\frac{1}{n}=0.a_1a_2\ \cdots a_m=\frac{[a_1a_2\ \cdots a_m]}{10^m}$$

ここで，$[a_1a_2\ \cdots a_m]$ とは

$$a_1\cdot 10^{m-1}+a_2\cdot 10^{m-2}+\ \cdots\ +a_m\cdot 10^0$$

のこととする．これより

$$n=\frac{10^m}{[a_1a_2\ \cdots a_m]}$$

左辺の n は整数なので，右辺も整数となる．したがって，$[a_1a_2\ \cdots a_m]$ は 10^m の約数であり，$[a_1a_2\ \cdots a_m]=2^p\cdot 5^q$ と表せ，したがって，$n=2^k\cdot 5^l$ と表せる．

これは，正の整数 a に対して a 進小数表示をするときには次のように拡張される．

Proposition 2. $a=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$ とするとき，自然数 n が

$$n=p_1^{l_1}p_2^{l_2}\cdots p_m^{l_m}$$

$$(\ l_i=0,1,2,\ \cdots\ ,i=0,\ 1,\ \cdots m\ )$$

ただし，すべての l_p が 0 ではないとする．

であるとき，$\dfrac{1}{n}$ の a 進法小数表示は有限小数となる．

逆に，$\dfrac{1}{n}$ が a 進法有限小数となるとすると，n は上記のように表すことができる．

Proof 2. $s=\max_{i=0,1,\cdots,m}\{p_i\}$ とすると

$$\frac{1}{n}=\frac{1}{p_1^{l_1}p_2^{l_2}\cdots p_m^{l_m}}=\frac{p_1^{s-l_1}p_2^{s-l_2}\cdots p_m^{s-l_m}}{a^s}$$

ここで，$p_1^{s-l_1}p_2^{s-l_2}\cdots p_m^{s-l_m}$ を a 進法表記したものを右詰にして左に 0 を補って $s-1$ 桁の数の列を作ったものを $[p_1^{s-l_1}p_2^{s-l_2}\cdots p_m^{s-l_m}]$ と表すこととすれば

$$\frac{1}{n}=0.\underbrace{[p_1^{s-l_1}p_2^{s-l_2}\cdots p_m^{s-l_m}]_{[a]}}_{k-1\text{ 桁}}$$

となり，a 進法有限小数となる．

逆に，$\dfrac{1}{n}$ が a 進法有限小数 $0.q_1q_2\ \cdots\ q_{k[a]}$ であるとすると

$$\frac{1}{n}=0.q_1q_2\ \cdots\ q_{k[a]}=\frac{[q_1q_2\ \cdots\ q_k]}{a^k}$$

ここで，$[q_1q_2\ \cdots\ q_k]$ とは

$$q_1\cdot a^{k-1}+q_2\cdot a^{k-2}+\ \cdots\ +q_k$$

のこととする．これより

$$\frac{a^k}{[q_1q_2\ \cdots\ q_k]}$$

左辺の n は整数なので，右辺も整数となる．したがって，$[q_1q_2\ \cdots\ q_k]$ は a^k の約数なので

$$[q_1q_2\ \cdots\ q_k]=p_1^{l_1}p_2^{l_2}\cdots p_m^{l_m}$$

という形になり，

$$n=p_1^{k_1-l_1}p_2^{k_2-l_2}\cdots p_m^{k_m-l_m}$$

とあらわすことができる．

4　混循環小数と純循環小数

小数第一位から循環する循環小数を純循環小数といい、小数第 m 位（$m\geqq 2$）から循環する循環小数を混循環小数という．

分数 $\dfrac{1}{n}$ が混循環小数であるとしよう．

$$\frac{1}{n}=0.s_1s_2\cdots s_{m-1}\dot{q}_1q_2\cdots\dot{q}_k$$

とすると

$$\frac{1}{n}=0.s_1s_2\cdots s_{m-1}+0.\underbrace{0\ 0\ \cdots\ 0}_{m-1\text{ 個}}\dot{q}_1q_2\cdots\dot{q}_k$$

$$=\frac{[s_1\ s_2\ \cdots\ s_{m-1}]}{10^{m-1}}+\frac{1}{10^{m-1}}\cdot 0.\dot{q}_1\ q_2\ \cdots\dot{q}_k$$

ここで,$x=0.\dot{q}_1\ q_2\ \cdots\dot{q}_k$ とすると

$$10^kx=q_1\ q_2\ \cdots q_k.\dot{q}_1\ q_2\ \cdots\dot{q}_k$$

$$x=0.\dot{q}_1\ q_2\ \cdots\dot{q}_k$$

より　$\left(10^k-1\right)x=[q_1\ q_2\ \cdots q_k]$

ただし，$[q_1\ q_2\ \cdots q_k]=q_1\cdot 10^{k-1}+q_2\cdot 10^{k-2}+\ \cdots\ +q_k$

したがって

$$\frac{1}{n}=\frac{[s_1\ s_2\ \cdots\ s_{m-1}]}{10^{m-1}}+\frac{1}{10^{m-1}}\cdot\frac{[q_1\ q_2\ \cdots\ q_k]}{10^k-1}$$

これより

$$n=\frac{10^{m-1}\cdot\left(10^k-1\right)}{\left(10^k-1\right)[s_1s_2\ \cdots\ s_{m-1}]+[q_1q_2\ \cdots\ q_k]}$$

左辺 n は整数であるから右辺も整数である．分母第 2 項の $[q_1q_2\ \cdots\ q_k]$ の約数は分母第 1 項と分子の 10^k-1 に同じ約数があるので，約分しても分子の 10^m がすべて約分されつくすことはないので，右辺は 10 を因数にもつ．したがって，n も因数 2 と因数 5 を持つ．n の因数 2 と因数 5 を取り尽くして

$$n=2^k\cdot 5^l\cdot n'$$

とすると，n' の中にはもう 2 や 5 の因数を持たないとしてよい．

したがって，$\dfrac{1}{n}$ が混循環小数であるときは，n はかならず因数 2 または因数 5 を持つことが示された．

対偶をとれば，n が 2, 5 の因数を持たなければ，$\dfrac{1}{n}$ は純循環小数であるということになる．　逆に，整数 n が因数として 2 または 5 を持つとき，すなわち $n=2^k\cdot 5^l\cdot n'$（n' は 10 と互いに素，$n'\neq 1$）と表されるとき，

(1) $k \geq l$ のとき

$$\frac{1}{n} = \frac{1}{2^k \cdot 5^l \cdot n'} = \frac{5^{k-l}}{10^k} \cdot \frac{1}{n'}$$

n' は因数として 2, 5 を含まないので $\frac{1}{n'}$ は純循環小数となり，後に第 8 節で示すように，$\frac{m}{n'}$ は $\frac{1}{n'}$ と同じ循環節の長さをもった純循環小数となる．したがって，$\frac{1}{10^k}$ によって循環節の始まりが k 個ずらされる．

(2) $k < l$ のとき

$$\frac{1}{n} = \frac{1}{2^k \cdot 5^l \cdot n'} = \frac{5^{l-k}}{10^l} \cdot \frac{1}{n'}$$

以下 (1) と同様にして示される．

以上より

Theorem 3. 正の整数 n に対して，$\frac{1}{n}$ を 10 進小数表示するとき，混循環小数となる必要十分条件は

$n = 2^k \cdot 5^l \cdot n'$　　n' は 10 と互いに素

（ k, l は 0 以上の整数とする．）

のときであり，このとき，$m = \max\{k, l\}$ とするとき，この混循環小数は小数第 m 位から循環節が始まる．

この定理は a 進法小数展開のときには次のようになる．

Theorem 4. a を 1 より大きい整数とし，$a = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ と素因数分解されるとする．ただし，p_1, p_2, $\cdots$ p_m は素数, k_1, k_2, $\cdots$ k_m は 0 以上の整数とする．

正の整数 n に対して，$\frac{1}{n}$ を a 進小数表示するとき，混循環小数となる必要十分条件は

$n = p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m} \cdot n'$　　n' は a と互いに素な正の整数

のときであり，このとき，$M = \max\limits_{p=1,2,\cdots,m} \{l_p\}$ とするとき，この混循環小数は小数第 M 位から循環節が始まる．

Proof 3. $\frac{1}{n}$ は混循環小数になるとする．

$$\frac{1}{n} = 0.s_1 s_2 \cdots s_{M-1} \dot{q_1} q_2 \cdots \dot{q_k}$$

とすると，

$$\begin{aligned}\frac{1}{n} &= 0.s_1 s_2 \cdots s_{M-1} + 0.\underbrace{00\cdots0}_{(M-1)\text{ 個}} \dot{q_1} q_2 \cdots \dot{q_k} \\ &= \frac{[s_1 s_2 \cdots s_{M-1}]}{a^{M-1}} + \frac{1}{a^{M-1}} \cdot 0.\dot{q_1} q_2 \cdots \dot{q_k} \\ &= \frac{[s_1 s_2 \cdots s_{M-1}]}{a^{M-1}} + \frac{1}{a^{M-1}} \cdot \frac{[q_1 q_2 \ \cdots \ q_k]}{a^k - 1}\end{aligned}$$

これより

$$n = \frac{a^{M-1} \cdot \left(a^k - 1\right)}{\left(a^k - 1\right)[s_1 s_2 \cdots s_{M-1}] + [q_1 q_2 \cdots q_k]}$$

左辺 n は整数であるから右辺も整数である．分母第 2 項の $[q_1 q_2 \ \cdots \ q_k]$ の約数は分母第 1 項と分子の $a^k - 1$ に同じ約数があるので，約分しても分子の a^{M-1} がすべて約分されつくすことはないので，右辺は a を因数にもつ．したがって，n も因数 $p_1, p_2, \cdots p_m$ を持つ．n の因数 $p_1, p_2, \cdots p_m$ を取り尽くして

$n = p_1^{l_1} p_2^{l_2} \ \cdots \ p_m^{l_m} \cdot n'$

とすると，n' の中にはもう因数 p_1, p_2, $\cdots$ p_m を持たないとしてよい．

したがって，$\frac{1}{n}$ が混循環小数であるときは，n はかならず因数 p_1, p_2, $\cdots$ p_m を持つことが示された．

対偶をとれば，n が因数 p_1, p_2, $\cdots$ p_m を持たなければ，$\frac{1}{n}$ は純循環小数であるということになる．

逆に, 整数 n が因数 p_1, p_2, $\cdots$ p_m を持つとき，すなわち　$n = p_1^{l_1} p_2^{l_2} \ \cdots \ p_m^{l_m} \cdot n'$（$n'$ は a と互いに素，$n' \neq 1$）と表されるとき，

$$M = \max_{p=1,2,\cdots,m} \{l_p\}$$

とすると

$$\frac{1}{n} = \frac{1}{p_1^{l_1} p_2^{l_2} \ \cdots \ p_m^{l_m} \cdot n'} = \frac{p_1^{k_1 - l_1} p_2^{k_2 - l_2} \ \cdots \ p_m^{k_m - l_m}}{a^{M-1} \cdot n'}$$

n' は a とは互いに素なので，$\frac{1}{n}$ は a 進小数では純循環小数隣，後に第 8 節で示すように $\frac{m}{n}$ は $\frac{1}{n}$ と同じ循環節の長さをもった純循環小数となる．したがって，$\frac{1}{a^M}$ によって循環節の始まりが M 個ずらされる．したがって，循環節は小数点第 M 位からはじまる．

5　循環節の長さ

第 2 節では，正整数 n に対して，$\frac{1}{n}$ を a 進小数展開をするとき，$1 \div n$ の計算途中で現れる商の列 $\{q_n\}$ と余りの列 $\{r_n\}$ について考えた．Theorem 1 は余りの列 $\{r_n\}$ が，

$r_n \equiv a^n \pmod{n}$

であることを示している．

a^n を n で割った余り r_n は，0, 1, 2, $\cdots$, $n-1$ の n 個のいずれかである．

$r_n = 0$ となるのは，a^n が n で割り切れるときであり，それはすなわち，$\frac{1}{n}$ が有限小数になるときである．3 節の Proposition 1, Proposition 2 で示したように，n が a の因数しか持たないときである．10 進小数を考えるときには，n が 2, 5 の因数を持たないときのことである．

このときには，r_n は 1, 2, $\cdots$, $n-1$ のいずれかである．$1 \div n$ を計算していくとき，$r_0 = 1$ であり，r_2, r_3, $\cdots$ と異なる余りが出るとしても，最大でも r_{n-2} までしか異なる余りが出続けることはできない．次の定理がなりたつ．

Theorem 5 (フェルマーの小定理)**.**

n は素数とし，a と n は互いに素とするとき

$$a^{n-1} \equiv 1 \pmod{n}$$

. $1\cdot a$ ， $2\cdot a$ ， $3\cdot a$ ， $\cdots$ $(n-1)\,a$ の $n-1$ 個について，$k\cdot a$ を n で割った商を Q_k，余りを R_k とする．すなわち

$$1\cdot a = Q_1 \times n + R_1$$
$$2\cdot a = Q_2 \times n + R_2$$
$$3\cdot a = Q_3 \times n + R_3$$
$$\cdots \quad \cdots$$
$$(n-1)\cdot a = Q_{n-1} \times n + R_{n-1}$$

とする．

このとき，これらの余り R_1, R_2, R_3, $\cdots$ R_{n-1} は全て異なる．

実際，$k\cdot a$ と $l\cdot a$ が同じ余りをもつとするならば

$$k\cdot a = Q_k \times n + R_k$$
$$l\cdot a = Q_l \times n + R_l$$

において，$R_k = R_l$ となるので，辺々引くことにより

$$(k-l)\cdot a = (Q_k - Q_l)\times n$$

となる．この式の右辺は n の倍数なので，左辺の $(k-l)\cdot a$ も n の倍数である．

ところが，a と n は互いに素であるので，このことから，$k-l$ が n の倍数となる．

ここで，$0 \le k \le n-1$，$0 \le l \le n-1$ なので，$-(n-1) \le k-l \le n-1$ なので，この $k-l$ が n の倍数であるということは，$k-l=0$ でなければならない．

したがって，$k=l$ となる．

そこで，これら $n-1$ 個の式を辺々かけあわせると

$$\begin{aligned} &1\cdot a \times 2\cdot a \times 3\cdot a \times \quad \cdots \quad (n-1)\cdot a \\ &= (Q_1 \times n + R_1) \\ &\quad \times (Q_2 \times n + R_2) \\ &\quad\quad \times (Q_3 \times n + R_3) \\ &\quad\quad\quad \times \cdots \quad \times (Q_{n-1} \times n + R_{n-1}) \\ &= Q \times n + R_1 \cdot R_2 \cdot R_3 \cdot \quad \cdots \quad \cdot R_{n-1} \end{aligned}$$

ここで，$n-1$ 個の R_1, R_2, $\cdots$, R_{n-1} は，すべて $0 \le R_k \le n-1$ であり，すべて異なるので，これらの積は

$$R_1 \cdot R_2 \cdot R_3 \cdot \quad \cdots \quad \cdot R_{n-1} = 1\cdot 2\cdot 3 \cdot \quad \cdots \quad \cdot (n-1)$$

となる．したがって

$$\begin{aligned} &1\cdot 2\cdot 3 \cdot \quad \cdots \quad \cdot (n-1) \times a^{n-1} \\ &\quad = Q \times n + 1\cdot 2\cdot 3 \cdot \quad \cdots \quad \cdot (n-1) \end{aligned}$$

となるので，

$$1\cdot 2\cdot 3 \cdot \quad \cdots \quad \cdot (n-1)\left(a^{n-1}-1\right) = Q \times n$$

この等式の右辺は n の倍数である．ところが，n は素数のときには，1, 2, 3, $\cdots$, $n-1$ は n と互いに素であるので，等式の左辺が n の倍数になることから

$$a^{n-1}-1 \quad \text{は} \quad n \text{の倍数} \qquad \text{すなわち}$$
$$a^{n-1} \equiv 1 \qquad (\bmod\ n)$$

この定理は次のように拡張される．

Theorem 6 (オイラー)**.**

a と n が互いに素であれば，オイラーの φ 関数を用いて

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

. $1\cdot a$ ， $2\cdot a$ ， $3\cdot a$ ， $\cdots$ $(n-1)\,a$ の $n-1$ 個について，$k\cdot a$ を n で割った商を Q_k，余りを R_k とする．すなわち

$$1\cdot a = Q_1 \times n + R_1$$
$$2\cdot a = Q_2 \times n + R_2$$
$$3\cdot a = Q_3 \times n + R_3$$
$$\cdots \quad \cdots$$
$$(n-1)\cdot a = Q_{n-1} \times n + R_{n-1}$$

とする．

このとき，これらの余り R_1, R_2, R_3, $\cdots$ R_{n-1} は全て異なる．

実際，$k\cdot a$ と $l\cdot a$ が同じ余りをもつとするならば

$$k\cdot a = Q_k \times n + R_k$$
$$l\cdot a = Q_l \times n + R_l$$

において，$R_k = R_l$ となるので，辺々引くことにより

$$(k-l)\cdot a = (Q_k - Q_l)\times n$$

となる．この式の右辺は n の倍数なので，左辺の $(k-l)\cdot a$ も n の倍数である．

ところが，a と n は互いに素であるので，このことから，$k-l$ が n の倍数となる．

ここで，$0 \le k \le n-1$，$0 \le l \le n-1$ なので，$-(n-1) \le k-l \le n-1$ なので，この $k-l$ が n の倍数であるということは，$k-l=0$ でなければならない．

したがって，$k=l$ となる．

また，k と n が 1 でない公約数 d を持つとき，$k\cdot a = Q_k \times n + R_k$ の左辺は d を約数にもち，右辺の $Q_k \times n$ も d を約数に持つので，R_k も d を約数にもつ．逆に k が d 約数に持たなければ，右辺の $Q_k \times n$ は d を約数に持つことから R_k は d を約数に持たない． そこで，これら n と互いに素になる k・・・ $\varphi(n)$ 個の式を辺々かけあわせると

$$\begin{aligned} &\underbrace{1\cdot a \times 2\cdot a \times 3\cdot a \times \quad \cdots \quad (n-1)\cdot a}_{n \text{ と互いに素となる } k} \\ &= (Q_1 \times n + R_1) \\ &\quad \times (Q_2 \times n + R_2) \\ &\quad\quad \times (Q_3 \times n + R_3) \\ &\quad\quad\quad \times \quad \cdots \quad \times (Q_{n-1} \times n + R_{n-1}) \\ &= Q \times n + \underbrace{R_1 \cdot R_2 \cdot R_3 \cdot \quad \cdots \quad \cdot R_{n-1}}_{n \text{ と互いに素となる } k} \end{aligned}$$

ここで，$n-1$ 個の R_1, R_2, $\cdots$, R_{n-1} は，すべて $0 \le R_k \le n-1$ であり，すべて異なるので，これらの積は

$$\underbrace{R_1 \cdot R_2 \cdot R_3 \cdot \ \cdots \ \cdot R_{n-1}}_{n \text{ と互いに素となる } k} = \underbrace{1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot (n-1)}_{n \text{ と互いに素となる } k}$$

となる．したがって

$$\underbrace{1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot (n-1)}_{n \text{ と互いに素となる } k} \times a^{\varphi(n)} = Q \times n + \underbrace{1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot (n-1)}_{n \text{ と互いに素となる } k}$$

となるので，

$$\underbrace{1 \cdot 2 \cdot 3 \cdot \ \cdots \ \cdot (n-1)}_{n \text{ と互いに素となる } k} \left(a^{\varphi(n)} - 1\right) = Q \times n$$

この等式の右辺は n の倍数である．ところが，n は素数のときには，$\underbrace{1,\ 2,\ 3,\ \cdots\ ,\ n-1}_{n \text{ と互いに素となる } k}$ は n と互いに素であるので，等式の左辺が n の倍数になることから

$a^{\varphi(n)} - 1$ は n の倍数　すなわち

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

例.

$a = 10,\ n = 21$ の場合，

$\frac{1}{n}$ の計算に現れる余りの列 $\{r_n\}$ は

$1 = n \times 0 + 1$　より　$r_0 = 1$

$10r_0 = 10 = 21 \times 0 + 10$　より　$r_1 = 10$

$10r_1 = 100 = 21 \times 4 + 16$　より　$r_2 = 16$

$10r_2 = 160 = 21 \times 7 + 13$　より　$r_3 = 13$

$10r_3 = 130 = 21 \times 6 + 9$　より　$r_4 = 4$

$10r_4 = 40 = 21 \times 1 + 19$　より　$r_5 = 19$

$10r_5 = 190 = 21 \times 9 + 1$　より　$r_6 = 1$

$r_6 = 1$ となったので，以下 r_1〜r_6 を繰り返す．そして，商も 0, 4, 7, 6, 1, 9 の順に繰り返すことになり，$\frac{1}{n}$ の小数展開は

$$\frac{1}{n} = 0.\dot{0}47619\dot{}$$

となる．

Theorem 1 あるいはその Corollary により，上のように決まる余りの数列 $\{r_k\}$ は

$r_k = 10^k$　あるいは　$r_k = r_1 \times r_{k-1}$

として求めることもできる．

$21 = 3 \times 7$ で 3 と 7 は互いに素なので $\varphi(21) = \varphi(3 \times 7) = \varphi(3) \times \varphi(7) = 2 \times 6 = 12$ であるから

$$a^{\varphi(21)} = a^{12} = \left(a^6\right)^2 = 1$$

となり，Theorem 6 は確かに成り立つ．

この場合，余りの集合 $\{r_n\}$ は $\{r_1,\ r_2,\ \cdots,\ r_6\}$ という 6 個の要素からなり，この 6 が循環節の長さでもある．

オイラーの定理 Theorem 6 は，循環節の長さは $\varphi(n)$ 以下であることを主張している．

上の例では，$\varphi(21) = 12$ であるのに，それよりも小さい $d = 6$ について

$$a^d \equiv 1 \pmod{n}$$

となっている．

この例のように $\varphi(n)$ より小さい d について，$a^d \equiv 1 \pmod{n}$ であれば，$k = 1$ から $k = d$ までを繰り返すことになる．したがって，$\varphi(n)$ は d の倍数である．

Theorem 7 (主定理)**.**
1 より大きい自然数 n, a に対して

(i) n と a が互いに素ではないとき

$\frac{1}{n}$ は a 進有限小数

(ii) n と a が互いに素であれば

$\frac{1}{n}$ は a 進循環小数となり

$a^d \equiv 1 \pmod{n}$ をみたす最小の自然数 d を考えると，この d が循環節の長さであり，d は $\varphi(n)$ の約数である．

6　循環節の長さ・・・n が素数の場合

「$a^d \equiv 1 \pmod{n}$ をみたす最小の自然数 d」はどのようにしてきまるのであろうか？

n が素数の場合を考えよう．正の自然数 a が因数として n を持つ場合には，$\frac{1}{n}$ は有限小数となるので，a と n は互いにその場合を考えることになる．

n が素数の場合，1 より小さい $1, 2, 3, \ \cdots\ , n-1$ は n と素になるので，

$$\varphi(n) = n - 1$$

となる．

n は素数なので $n-1$ は偶数であり，$\frac{n-1}{2}$ は整数となり，

$$a^{n-1} - 1 = \left(a^{\frac{n-1}{2}} + 1\right)\left(a^{\frac{n-1}{2}} - 1\right) \equiv 0 \pmod{n}$$

ここで，もしも $a^{\frac{n-1}{2}} - 1 \equiv 0 \pmod{n}$ が成り立つようであれば，

$\varphi(n) = n - 1$ より小さい整数 m で

$$a^m \equiv 1 \pmod{n}$$

を成り立たせるものが存在することになる．$\frac{n-1}{2}$ が偶数であれば，同じように和と差の席に素因数分解されてさらに小さい m が存在する可能性がある．

また，$\frac{n-1}{2}$ が奇数の場合には，$\frac{n-1}{2} = 2k - 1$ であれば

$$a^{2k-1} - 1 = (a-1)\left(a^{2k-2} + a^{2k-3} + \ \cdots\ + a + 1\right) \equiv 0 \pmod{n}$$

$a - 1 \equiv 0 \pmod{n}$ でなければ

$$a^{2k-2} + a^{2k-3} + \ \cdots\ + a + 1 \equiv 0 \pmod{n}$$

このように，$a^{n-1} - 1$ を素因数分解したときの各因数

の中で $a^d-1\equiv 0\ ,\ \pmod n$ となる最小の d を探すことにより，これを満たす最小の d すなわち $\dfrac{1}{n}$ の循環節の長さを求めることができる．

例えば，$n=13,\ a=10$ の場合を考えてみよう．

$$\begin{aligned}&10^{13-1}-1=10^{12}-1\\&=\left(10^6+1\right)\left(10^6-1\right)\\&=\left(10^2+1\right)\left(10^4-10^2+1\right)\times\\&\quad\times(10+1)\left(10^2-10+1\right)\times\\&\quad\times(10-1)\left(10^2+10+1\right)\end{aligned}$$

ここで

$10^2+1=101$　これは　素数

$10^4-10^2+1=9901$　これは　素数

ゆえに　$10^6+1\not\equiv 0\ ,\ \pmod{13}$

$10+1=11$　これは素数

$10^2-10+1=91=7\times 13$

したがって　$10^2-10+1\equiv 0$　$\therefore\ 10^3+1\equiv 0$

$10-1=9=3^2$　これは素数

$10^2+10+1=111=3\times 37$

したがって　$10^2+10+1\equiv 0$　$\therefore\ 10^3-1\not\equiv 0$

したがって　$\therefore\ 10^6-1\equiv 0$

これから　$a^m\equiv 1\ \pmod n$ をみたす最小の m は 6

$\therefore d=6$

実際に

$$\frac{1}{13}=0.\dot{0}76923\dot{}$$

であり $\dfrac{1}{13}$ の循環節の長さは 6 である．

7　Midy の定理の証明・・・その 1

a は正の整数, n は素数とする．$\dfrac{1}{n}$ を a 進法小数展開したときに循環節の長さが偶数 $2m$ であると仮定する．このとき，循環節の最初の m 個を右詰に並べてできる m 桁の整数を A とし，最後の m 個によってできる m 桁の整数を B とするとき

$$A+B=a^m-1$$

となる．ただし，m 個のなかの先頭のいくつかが 0 であるときはには必ずしも m 桁とはなるとは限らない．

$\dfrac{1}{n}$ を a 進法小数展開したときに循環節の長さが偶数 $2m$ であることから，

$$a^{2m}\equiv 1\ \pmod n$$

であり，

$2m$ より小さい正の整数 l に対しては

$$a^l\not\equiv 1\ \pmod n$$

である．

$$a^{2m}-1=\left(a^m+1\right)\left(a^m-1\right)\equiv 0\ \pmod n$$

であるけれども，$a^m-1\not\equiv 0\ \pmod n$　なので

$a^m+1\equiv 0$　すなわち　$a^m\equiv -1\ \pmod n$

さて，A は第 2 節でみたように，a^m を n で割ったときの商であり，そのときの余りは $n-1$ となる．

$$a^m=A\times n+(n-1)\qquad(1)$$

さらに，B はこの余り $n-1$ から割り算を初めた m 個を並べたものであるので

$$(n-1)\,a^m=B\times n+1\qquad(2)$$

という関係がある．

$(1)+(2)$ とすると

$$n\times a^m=(A+B)\times n+n$$

これから　$A+B=a^m-1$

が成り立つ．

特に $a=10$ のときには，

$$a^m-1=10^m-1=\underbrace{999\ \cdots\ 99}_{m\text{ 個}}$$

であるので，分子が 1 である $\dfrac{1}{n}$ についての Midy の定理が証明された．

Midy の定理の主張する性質は，以下に示すように，前提とする条件を若干弱めたうえでより強い性質が主張できることが証明できる．

Theorem 8. a は正の整数, n は素数とする．$a^d+1\equiv 0\ \pmod n$ をみたす n より小さい正の整数 d が存在して，$2d$ より小さい l に対しては $a^l\not\equiv 1$ が成り立てば，$\dfrac{1}{n}$ を a 進法小数展開したときに循環節の長さが偶数 $2d$ であり，このとき，$1\leqq k\leqq d$ を満たす任意の整数 k について，循環節の第 k 番目の数を A とし，第 $d+k$ 番目の数を B とするとき

$$A+B=a-1$$

となる．

Proof 4. $a^d+1\equiv 0\ \pmod n$ をみたす n より小さい正の整数 d が存在すると仮定する．このとき

$$a^{2d}-1=\left(a^d+1\right)\left(a^d-1\right)\equiv 0\ \pmod n$$

が成り立ち，$2d$ より小さい l に対しては $a^l\not\equiv 1$ であるので，この $2d$ が $a^m\equiv 1\ \pmod n$ をみたす最小の整数となるので，循環節の長さは $2d$ である．

このとき，$1\leqq k\leqq d$ に対しては，$a^k\not\equiv 1\ \pmod n$ であるので，

$$\begin{aligned}&a^1=q_1\times n+r_1\\&a^2\equiv a\times r_1=q_2\times n+r_2\\&\cdots\qquad\cdots\qquad\cdots\\&a^d\equiv a\times r_{d-1}=q_d\times n+r_d\end{aligned}$$

となるときの $r_1,\ r_2,\ \cdots,\ r_{d-1}$ はすべて異なり，± 1 とも異なり，$r_d\equiv -1\ \pmod n$ より　$r_d=n-1$ である．そして，

$$\begin{aligned}&a^{d+1}\equiv a\times r_d=q_{d+1}\times n+r_{d+1}\\&a^{d+2}\equiv a\times r_{d+1}=q_{d+2}\times n+r_{d+2}\\&\cdots\qquad\cdots\qquad\cdots\\&a^{2d}\equiv a\times r_{2d-1}=q_{2d}\times n+r_{2d}\end{aligned}$$

となるとき，

$$\begin{aligned}&r_{d+1}\equiv r_d\times r_1=-1\times r_1=n-r_1\\&r_{d+2}\equiv r_d\times r_2=-1\times r_2=n-r_2\end{aligned}$$

・・・　　・・・　　・・・

$r_{d+d} \equiv r_d \times r_d = -1 \times r_d = n - r_d$

となるので

$r_k + r_{d+k} = r_k + (n - r_k) = n$

であり,

$a_k + a_{d+k} = (q_k + q_{d+k}) \times n + (r_k + r_{d+k})$

$= (q_k + q_{d+k}) \times n + n$

ここで,

$a^k + a^{d+k} = a^k + a^k \cdot a^d = a^k \left(1 + a^d\right)$

なので

$a^k + a^{d+k} \equiv (q_k + q_{d+k}) \times n + n$

より

$\dfrac{a^d + 1}{n} \cdot a^k = q_k + q_{d+k} + 1$

ここで, $a^d + 1 \equiv 0 \pmod{n}$ より　$\dfrac{a^d + 1}{n}$ は整数である. また,

$0 \leqq q_k \leqq a - 1,\ 0 \leqq q_{d+k} \leqq a - 1$

より　$-1 \leqq q_k + q_{d+k} \leqq 2a - 1$　なので, これより

$q_k + q_{d+k} + 1 = a$　ゆえに　$q_k + q_{d+k} = a - 1$

Midy の定理の主張するのは

「循環節の最初の m 個を右詰に並べてできる m 桁の整数を A とし, 最後の m 個によってできる m 桁の整数を B とするとき

$A + B = a^m - 1$

となる.」

ことであったが, 実際には 2 分割した 2 つの整数 A, B の対応する各桁の数 a, b について

$a + b = a - 1$

が成り立つことがわかった. この強い意味での性質を「Midy の性質」と呼ぶこととする.

8　n が素数のときの $\dfrac{m}{n}$ の循環節

n が素数で, 正の整数 a と n は互いに素とする. このとき, $\varphi(n) = n - 1$ であり, $\dfrac{1}{n}$ の a 進小数表示は循環節の長さが d の循環小数となる. このとき d は $\varphi(n) = n - 1$ の約数となっており, $a^d \equiv 1 \pmod{n}$ となる.

$\dfrac{1}{n}$ を a 進小数表示するための $1 \div n$ の計算に現れる商 q_k と余り r_k を考える.

a^k を n で割ったときの商が q_k, 余りが r_k であり

$a = q_1 \times n + r_1$

$a^2 = q_2 \times n + r_2$　　$a^2 \equiv a \times r_1 \pmod{n}$

・・・　　・・・　　・・・

$a^k = q_k \times n + r_k$　　$a^k \equiv a \times r_{k-1} \pmod{n}$

・・・　　・・・　　・・・

$a^d = q_d \times n + r_d$　　$a^k \equiv a \times r_{k-1} \pmod{n}$

となっている. このとき,

$R_a(n) = \{r_k\}$　　$r_k \equiv a^k \pmod{n}$

$Q_a(n) = \{q_k\}$

循環節の長さが d であることから, $r_1,\ r_2,\ \cdots,\ r_d$ はみな異なり, $r_d = 1$ であり, したがって $R_a(n)$ は d 個の要素をもつ有限集合である.

$a = 10,\ n = 7$ のときの $\dfrac{1}{n}$ を見てみよう

$$
\begin{array}{r|l}
 & 0.\ 1\ 4\ 2\ 8\ 5\ 7 \\
\hline
7 & 1\ 0 \\
 & \ \ 7 \\
\hline
 & \ \ 3 \qquad \Longleftarrow r_1 \\
 & \ 2\ 8 \\
\hline
 & \ \ \ 2\ 0 \qquad \Longleftarrow r_2 \\
 & \ \ \ 1\ 4 \\
\hline
 & \ \ \ \ 6\ 0 \qquad \Longleftarrow r_3 \\
 & \ \ \ \ 5\ 6 \\
\hline
 & \ \ \ \ \ 4\ 0 \qquad \Longleftarrow r_4 \\
 & \ \ \ \ \ 3\ 5 \\
\hline
 & \ \ \ \ \ \ 5\ 0 \qquad \Longleftarrow r_5 \\
 & \ \ \ \ \ \ 4\ 9 \\
\hline
 & \ \ \ \ \ \ \ 1 \qquad \Longleftarrow r_6
\end{array}
$$

この場合,

$r_1 = 3,\ r_2 = 2,\ r_3 = 6,\ r_4 = 4,\ r_5 = 5,\ r_6 = 1$

となる.

このとき, $\dfrac{3}{n}$ の小数展開を求めると

$$
\begin{array}{r|l}
 & 0.\ 4\ 2\ 8\ 5\ 7\ 1 \\
\hline
7 & 3\ 0 \\
 & \ 2\ 8 \\
\hline
 & \ \ \ 2\ 0 \\
 & \ \ \ 1\ 4 \\
\hline
 & \ \ \ \ 6\ 0 \\
 & \ \ \ \ 5\ 6 \\
\hline
 & \ \ \ \ \ 4\ 0 \\
 & \ \ \ \ \ 3\ 5 \\
\hline
 & \ \ \ \ \ \ 5\ 0 \\
 & \ \ \ \ \ \ 4\ 9 \\
\hline
 & \ \ \ \ \ \ \ 1\ 0 \\
 & \ \ \ \ \ \ \ \ 7 \\
\hline
 & \ \ \ \ \ \ \ \ 3
\end{array}
$$

となる.

$\dfrac{1}{n}$ の計算で $r_1 = 3$ が出たところから計算が始まる, 同じ余りが出ると, そこから先は $\dfrac{1}{n}$ の計算と同じことを繰り返していき, $r_1,\ r_2,\ \cdots,\ r_6$ と同じ順に余りが決まっていき, それに対応して商 $q_1,\ q_2,\ \cdots,\ q_6$ と同じ順で商も決まっていく.

一般に, $\dfrac{m}{n}$ の小数展開を考えよう.

$m > n$ のときには帯分数に直して整数部分を除いた分数の小数展開を考えることになるので, $m < n$ と仮定しても一般性を失わない.

m を n で割ったときの商を q_0, 余りを r_0 とすると,

$m = q_0 \times n + r_0$

実際には　$m < n$ と仮定すると　$q_0 = 0,\ r_0 = m$ である. この後

$a \times r_0 = q_1 \times n + r_1$

$a \times r_1 = q_2 \times n + r_2$

$$\cdots \qquad \cdots \qquad \cdots$$
$$a \times r_{k-1} = q_k \times n + r_k$$
$$\cdots \qquad \cdots \qquad \cdots$$
$$a \times r_{d-1} = q_d \times n + r_d$$

となり，$r_{k+1} = a \times r_k$ という漸化式は $\dfrac{1}{n}$ のときと同じである．

したがって，$\dfrac{m}{n}$ を a 進小数表示するときにあらわれる余りの作る集合は

$$mR_a(n) \equiv \{m \times r_1,\ m \times r_2,\ \cdots,\ m \times r_d\} \pmod{n}$$

となる．

$r_1,\ r_2,\ \cdots,\ r_d$ はすべて異なることから，$m \times r_1,\ m \times r_2,\ \cdots,\ m \times r_d$ もすべて異なり，$m \times r_d = r \times 1 = m$ となる．

このことから，$(n-1)$ 個集合 $mR_a(n)$，$m = 1, 2, \cdots, n-1$ のうち，異なる集合は $\dfrac{n-1}{d}$ 個あることになる．

例 1. $a = 10,\ n = 7$ のときの $\dfrac{1}{n}$ については

$n = 7$ は素数なので $\varphi(n) = n - 1 = 6$

$$1 = 0 \times 7 + 1 \quad \Longrightarrow \quad 10 \times 1 = 1 \times 7 + 3$$
$$10 \times 3 = 4 \times 7 + 2 \quad \Longrightarrow \quad 10 \times 2 = 2 \times 7 + 6$$
$$10 \times 6 = 8 \times 7 + 4 \quad \Longrightarrow \quad 10 \times 4 = 5 \times 7 + 5$$
$$10 \times 5 = 7 \times 7 + 1$$

となるので，$10^d \equiv 1 \pmod{n}$ となる最小の整数 d は

$$d = 6$$

$\dfrac{n-1}{d} = 1$ なので分子 m が $1, 2, 3, 4, 5, 6$ のいずれの時でも余りに現れる数はみな同じになる．　$R_{10}(7) = \{3, 2, 6, 4, 5, 1\}$ であり

$$R_{10}(7) = 3R_{10}(7) = 2R_{10}(7) = 6R_{10}(7) = 4R_{10}(7) = 5R_{10}(7)$$

したがって，循環節を作る数の並びも，以下のように先頭が異なるだけでようにすべて同じになる．

$$\frac{1}{7} = 0.\dot{1}42857\dot{} \quad \frac{3}{7} = 0.\dot{4}28571\dot{} \quad \frac{2}{7} = 0.\dot{2}85714\dot{}$$
$$\frac{6}{7} = 0.\dot{8}57142\dot{} \quad \frac{4}{7} = 0.\dot{5}71428\dot{} \quad \frac{5}{7} = 0.\dot{7}14285\dot{}$$

例 2. $a = 10,\ n = 41$ のときの $\dfrac{1}{n}$ を見てみよう

$n = 41$ は素数なので $\varphi(n) = n - 1 = 40$

$$1 = 0 \times 41 + 1 \quad \Longrightarrow \quad 10 \times 1 = 0 \times 41 + 10$$
$$10 \times 10 = 2 \times 41 + 18 \quad \Longrightarrow \quad 10 \times 18 = 4 \times 41 + 16$$
$$10 \times 16 = 3 \times 41 + 37 \quad \Longrightarrow \quad 10 \times 37 = 9 \times 41 + 1$$

となるので，$10^d \equiv 1 \pmod{n}$ となる最小の整数 d は

$$d = 5$$

$R_{10}(41) = \{10, 18, 16, 37, 1\}$ であり，

$$R_{10}(41) = 10R_{10}(41) = 18R_{10}(41) = 16R_{10}(41) = 37R_{10}(41)$$

$$\frac{1}{41} = 0.\dot{0}2439\dot{} \quad \frac{10}{41} = 0.\dot{2}4390\dot{} \quad \frac{18}{41} = 0.\dot{4}3902\dot{}$$
$$\frac{16}{41} = 0.\dot{3}9024\dot{} \quad \frac{37}{41} = 0.\dot{9}0243\dot{}$$

$2R_{10}(41) = \{20, 36, 32, 33, 2\}$ であり，

$$2R_{10}(41) = 20R_{10}(41) = 36R_{10}(41) = 32R_{10}(41) = 33R_{10}(41)$$
$$\frac{2}{41} = 0.\dot{0}4878\dot{} \quad \frac{20}{41} = 0.\dot{4}8780\dot{} \quad \frac{36}{41} = 0.\dot{8}7804\dot{}$$
$$\frac{32}{41} = 0.\dot{7}8048\dot{} \quad \frac{33}{41} = 0.\dot{8}0487\dot{}$$

$3R_{10}(41) = \{30, 13, 7, 29, 3\}$ であり，

$$3R_{10}(41) = 30R_{10}(41) = 13R_{10}(41) = 7R_{10}(41) = 29R_{10}(41)$$

であり，

$$\frac{3}{41} = 0.\dot{0}7317\dot{} \quad \frac{30}{41} = 0.\dot{7}3130\dot{} \quad \frac{13}{41} = 0.\dot{3}1707\dot{}$$
$$\frac{7}{41} = 0.\dot{1}7073\dot{} \quad \frac{29}{41} = 0.\dot{7}0731\dot{}$$

同様に，$4R_{10}(41) = \{40, 31, 23, 25, 4\}$ であり，

$$4R_{10}(41) = 40R_{10}(41) = 31R_{10}(41) = 23R_{10}(41) = 25R_{10}(41)$$

となり

$$\frac{4}{41},\ \frac{40}{41},\ \frac{31}{41},\ \frac{23}{41},\ \frac{25}{41}$$

の循環節に並ぶ数字は一つずつずれるけれども同じものが同じ順に並ぶ．

以下同様に，

$$5R_{10}(41) = \{9, 8, 39, 21, 5\}$$
$$6R_{10}(41) = \{19, 26, 14, 17, 6\}$$
$$7R_{10}(41) = \{29, 3, 30, 13, 7\}$$
$$11R_{10}(41) = \{28, 34, 12, 38, 11\}$$
$$15R_{10}(41) = \{27, 24, 35, 22, 15\}$$

である．

$\dfrac{m}{41}$ という 40 個の分数は，$40 \div 5 = 8$ 組ずつが同じ余りの数列から循環節が決まる．

9 $\dfrac{1}{n_1 \times n_2}$ の小数展開

$\dfrac{1}{n_1 \times n_2}$ の循環節の長さを d とすると

$$a^l \equiv 1 \pmod{n_1 \times n_2}$$

をみたす最小の l が d である．

$a^d = n_1 \times n_2 \times Q + 1$　であるから，

$$a^d = n_1 \times n_2 Q + 1$$
$$a^d = n_2 \times n_1 Q + 1$$

より　$a^d \equiv 1 \pmod{n_1}$　かつ　$a^d \equiv 1 \pmod{n_2}$

である．

n_1 と n_2 が互いに素であるとき，$\dfrac{1}{n_1}$ の循環

節の長さを d_1, $\dfrac{1}{n_2}$ の循環節の長さを d_2 とする．すなわち

$a^l \equiv 1 \pmod{n_1}$　をみたす最小の l が d_1

$a^l \equiv 1 \pmod{n_2}$　をみたす最小の l が d_2

である．このとき，d_1 と d_2 の最小公倍数を L とする．

$L = d_1 \times m_1$，$d_2 \times m_2$　とすると

$a^L = \left(a_1^d\right)^{m_1} \equiv 1 \pmod{n_1}$

$a^L = \left(a_2^d\right)^{m_2} \equiv 1 \pmod{n_2}$

となるので，

$a^L = n_1 \times Q_1 + 1$

となり，さらに Q_1 を　$Q_1 = n_2 \times Q_1' + R_1$ とすると

$a^L = n_1 \times n_2 \times Q_1' + n_1 \times R_1 + 1$　　(1)

同様に

$a^L = n_2 \times Q_2 + 1$

となり，さらに Q_2 を　$Q_2 = n_1 \times Q_2' + R_2'$ とすると

$a^L = n_1 \times n_2 \times Q_2' + n_2 \times R_2 + 1$　　(2)

(1) − (2) とすると

$0 = n_1 \times n_2 \times (Q_1' - Q_2') + n_1 \times R_1 - n_2 \times R_2$

したがって　$n_1 \times R_1 = n_2 \times R_2 - n_1 \times n_2 \times (Q_1' - Q_2')$

となり，n_1 と n_2 が互いに素であることから，R_1 は n_2 で割り切れることがわかる．これより

$a^L \equiv 1 \pmod{n_1 \times n_2}$

である．

ここで，$d > L$ と仮定すると

$a^d \equiv 1 \pmod{n_1 \times n_2}$

$a^L \equiv 1 \pmod{n_1 \times n_2}$

より　$a^d - a^L = \left(a^{d-L} - 1\right) a^d \equiv 0 \pmod{n_1 \times n_2}$

$a^d \equiv 1$ より $a^{d-L} - 1 \equiv 1$

$d - L < L$ でなくても，同様に繰り返すと有限回で $d - L < L$ となる．これは L の最小性に矛盾する．

したがって $d = L$ である．

以上のことから，次の定理を得る．

Theorem 9. n_1 と n_2 が互いに素であるとき，$\dfrac{1}{n_1}$ の循環節の長さを d_1，$\dfrac{1}{n_2}$ の循環節の長さを d_2 とすると $\dfrac{1}{n_1 \times n_2}$ の循環節の長さ d は

$d = \mathrm{LCM}\,(d_1, d_2)$

n_1 と n_2 が互いに素でないとき，例えば p を素数として $n_1 = n_2 = p$ のときには，$\dfrac{1}{p}$ の循環節の長さを d とすると，$\dfrac{1}{p^2}$ の循環節の長さは

$p \times d$

となるという予想を持っている．

例 3.

(1)　$\dfrac{1}{7}$ の循環節の長さは 6 であり

$\dfrac{1}{7^2}$ の循環節の長さは $42 = 7 \times 6$ である．

(2)　$\dfrac{1}{13}$ の循環節の長さは 6 であり

$\dfrac{1}{13^2}$ の循環節の長さは $78 = 13 \times 6$ である．

(3)　$\dfrac{1}{37}$ の循環節の長さは 3 であり

$\dfrac{1}{37^2}$ の循環節の長さは $111 = 13 \times 3$ である．

例 4. (1) $\dfrac{1}{21} = \dfrac{1}{3 \times 7}$ の循環節について

$\dfrac{1}{3 \times 7} = 0.\dot{0}47619\dot{}$ であり，Midy の定理の条件「循環節の長さが偶数 $2d$」を満たしている．もちろん分母は素数でなくて合成数であるが，循環節の前半を $A = 047$, 後半を $B = 619$ とすると

$A + B = 047 + 619 = 666$

となり，999 ではないが，6 が 3 つ並ぶ．

これについては，次のような計算が何か秘密を解く鍵かもしれないと考えている．

$1000 = 21 \times A + 13 = 21 \times 47 + 13$　　(1)

$13 \times 1000 = 21 \times B + 1 = 21 \times 619 + 1$　　(2)

(1) + (2) とすると

$(1 + 13) \times 1000 = 21 \times (A + B) + (13 + 1)$

$\dfrac{(A + B) \times 3}{2} = 1000 - 1$

これより　$A + B = \dfrac{2 \times 999}{3}$

$A + B$ ではなくて，桁ごとに加えて 9 になる性質を「Midy の強性質」といったが，これは桁ごとでは成り立たないが $A + B$ が全体として 666 になるという意味で「Midy の弱性質」である．

この現象は $A + B = \dfrac{2 \times 999}{3}$ が整数になるようになればよいので，999 の約数との関係になると考えている．

(2) $\dfrac{1}{259} = \dfrac{1}{7 \times 37}$ の循環節について

$\dfrac{1}{7 \times 37} = 0.\dot{0}03861\dot{}$ であり，循環節の長さが 6 である．

$1000 = 259 \times A + 158 = 259 \times 003 + 158$　(3)

$158 \times 1000 = 259 \times B + 1 = 259 \times 61 + 1$　(4)

(3) + (4) とすると

$(1 + 158) \times 1000 = 259 \times (3 + 61) + (158 + 1)$

$159 \times 1000 = 259 \times 64 + 159$

ここで，$224 = 2^5 \times 7$　$999 = 3^3 \times 37$　$259 = 7 \times 37$

より　$A + B = \dfrac{224 \times 999}{259} = 2^5 \times 3^3$

これより　$A + B = 864$

まだまだ興味深い現象があるようである．

10　参考文献

[1]E.Midy 1836,

De Quelques Proprieies des Numbres et des Fractions Decimales Periodiques,Nantes,1836