数学の研究を始めよう (2)
誕生日を遊ぶ

飯高 茂

平成 25 年 7 月 17 日

1　誕生日

私の誕生日は 5 月 29 日である. 5 と 29 はともに素数だが 529 は素数でない. 実際 ,$529 = 23^2$ と因数分解できる.

p 月 q 日 とするとき p, q がともに素数でかつ $100p + q$ が素数の平方になる p, q は 5,29 しかない. 自分の誕生日の数学的特徴付けができた.

ところで 529 を置換のサイクル (5 2 9) とみてこれに互換 $(1, 2)$ を作用させる (簡単にいえば最初と次の数を入れ替えると) と結果として 259 となる. これを素因数分解すると $7 \cdot 37$ になる.

$\frac{1}{7}$ と $\frac{1}{37}$ はとても気のきいた分数なのである. 実際,10 進小数で展開すると,

$$\frac{1}{7} = 0.14285714285714285\cdots$$

このとき小数点の次から 142857 が繰り返される. すなわちこれは循環小数である. この場合は初めから循環するので純循環する, という. また 142857 を循環節と言う. これは 6 個の数からなるので循環節の長さは 6 と言う.

循環節 142857 を 2 分割すると 142 と 857 になる. これを加えると $142 + 857 = 999$ となる. よって 142857 の 2 分割和は 999 になるという.

次に循環節を 3 分割すると 14 と 28 と 57 をえるがこれらを加えると $14 + 28 + 57 = 99$. また 9 がでてきた. これを 142857 の 3 分割和は 99 になるという.

さて分子を変えてみると

$$\frac{3}{7} = 0.42857142857142857\cdots$$

となって,$\frac{3}{7}$ の循環節は 428571 となることがわかる.

この循環節 428571 を 3 分割すると 42 と 85 と 71 をえるがこれらを加えた 3 分割和は $42 + 85 + 71 = 198 = 2 \times 99$. これは 99 の 2 倍である. 99 にならないところが面白い. これは新しく興味ある発見の端緒なのである.

1.1　素数分の 1

分母が素数 $p(\neq 2, 5)$ の場合に $\frac{1}{p}$ の循環節の長さが偶数の時その 2 分割和は 9 が並ぶ. これは古くから知られていた事実で, このことを西欧で 2 番目に書いたフランスの数学者 Midy の名前をとって **Midy の定理**という.

たとえば $\frac{1}{17}$ の計算をしてみよう.

$$\frac{1}{17} = 0.058823529411764705\cdots$$

05 が繰り返しの端緒であって循環節は 0588235294117647, 長さは 16. 循環節を 2 分割して加えると

$$05882352 + 94117647 = 99999999$$

$\frac{1}{19}$ は 052631578947368421 が循環節であって 2 分割すると 052631578 と 947368421 になる. これを加えると

$$052631578 + 947368421 = 999999999$$

長さは $19 - 1 = 18$ なので 3 分割できて 052631 と 578947 と 368421 になる.

表 1: $\frac{1}{19}$ の循環節の 3 分割和

	052631
	578947
+)	368421
	999999

$\frac{1}{29}$ の循環節は 034482758620689655172413793l, 長さは 28. 2 分割和,4 分割和,7 分割和ができる. 自分でやってみよう.

$\frac{1}{5}$ の 10 進展開は 0.2 になるだけでこれはつまらない. この場合, 分母が 5 なので 10 進展開が面白くならない.

$g = 7$ にとって $\frac{1}{5}$ を 7 進展開してみよう.

このとき 1254 が循環節なのだが 2 分割和は $12 + 54 = 66$ となる.

$6 = 7 - 1$ なので 7 進展開では 6 の並ぶことが多い.

$\frac{1}{11} = 0.0909\cdots$ はつまらない展開なのだが,7 進展開すると断然面白くなる.

$\frac{1}{11}$ の 7 進展開の循環節は 0431162355. 2 分割和をしてみよう. 6 が並ぶ.

$\frac{1}{13}$ の 7 進展開の循環節は 035245631421. この 2 分割和と 3 分割和を計算してみると 6 が並ぶ. 足し算で繰り上がりがあるので 7 進数展開の和にうまく 6 が並ぶ.

一般に 正の整数 $g > 1$ を決めて g 進展開するとき分母が g と互いに素という条件を課すことが必要になる. そうすると既約分数の g 進展開は必ず純循環するのである.

1.2 1/259 の不思議

分母が 259 の分数を 10 進展開すると

$$\frac{1}{259} = 0.003861003861003861\cdots$$

したがって 循環節 003861 をえる. これを 2 分して足す. $3+861=867$. 面白くないな. 足してダメなら引いてみよう. 大きい方から小さい方を引く. $861-3=858$. これからさらに 1 を引くと 857.

分子が 123 のとき $\frac{123}{259}$ の循環節は 474903. この 2 分割差から 1 を引くと $903-474-1=428$.

857 や 428 を見て $\frac{1}{7}$ の循環節の一部だとわかる人はすごい眼力の持ち主である.

分母が 259 で,7 または 37 で割れない数が分子のときその分数の循環節は 6 桁からなる. この循環節の 2 分割差は次の通り.

表 2: $\frac{a}{259}$ の循環節の 2 分割差

分数	2 分割差	2 分割差 -1
1/259	[8,5,8]	[8,5,7]
2/259	[7,1,5]	[7,1,4]
3/259	[5,7,2]	[5,7,1]
4/259	[4,2,9]	[4,2,8]
5/259	[2,8,6]	[2,8,4]
6/259	[1,4,3]	[1,4,2]
8/259	[8,5,8]	[8,5,7]

以後は繰り返しになる.

$\frac{a}{259}$ の循環節の 2 分割差 -1 として $\frac{1}{7}$ の循環節の半分がひょこひょこ出てくるのは実に面白い.

1.3 1/37 の不思議

$\frac{1}{37}$ の循環節は 027 でありその長さは 3 である.3 分割して加えると $0+2+7=9$.

高等学校の数学 I で, 有理数を小数に展開して循環することを確かめる例が出ているが分母が 37 の分数を例題にとっていることが多い. 実は循環節の長さが 3 の分数は分母が 37 の分数に限るのである.

ちなみに, 循環節の長さが 5 の分数は分母が 41, または 271.

$529=23^2$ に由来する分数を計算しよう.

$\frac{1}{23}$ の 循環節の長さは 22, 循環節自身は 0434782608695652173913. 2 分割して足すと次の通り.

表 3: $\frac{1}{23}$ の循環節の 2 分割和

$$\begin{array}{rr} & 04347826086 \\ +) & 95652173913 \\ \hline & 99999999999 \end{array}$$

$\frac{1}{529}$ の循環節の長さは $22\times 23=506$. 2 分割して足すと 9 が 253 個の並ぶ.

素数 $p > 2$ に対してそのべき p^r を法とする剰余群は巡回群である. この性質がものを言って, 分母が p^r の分数の 10 進展開の循環節の 2 分割和は 9 が並ぶ.

しかし法が 2 べき 2^r のときは $r > 2$ なら剰余群は巡回群にならない. 2^{r-2} 次の巡回群と 2 次の巡回群の直積になってしまう. ここに, 奇素数と 2, すなわち唯一の偶素数の違いがある.

1.4 1 月 28 日

私の長男は 1 月 28 日 生まれなので $128 = 2^7$ に注意しつつ $\frac{1}{128}$ を 5 進数展開するその循環節は実に面白い性質を持っている. その循環節の長さは 32 であり, 並べると

00044201334330402232142411210313

これは扱いが難しいのでもっと簡単な $\frac{1}{32}$ を 5 進数展開してみよう. その循環節は 00342312. この 5 進数としての 2 分割和は 2401. 2 分割差は 2223 となりきれい.

$\frac{1}{64}$ を 5 進数展開するとその循環節は 0014340322421131.
2 分割差を 5 進数として計算してみよう.

表 4: 2 分割差

	2	2	4	2	1	1	3	1
−)	0	0	1	4	3	4	0	3
	2	2	2	2	2	2	2	3

1.5 7 進数展開の例

$\frac{1}{128}$ を 7 進数展開するとその循環節は 0024520633611543 になる.
この 2 分割差を 7 進数として計算してみてください.
2 のべきに小さい数が掛けられている場合も 2 分割差は美しい性質を持つ. 実際,
$\frac{1}{3 \times 128}$ を 7 進数展開するとその循環節は 0006152433425161 になる.
この 2 分割差を 7 進数として計算してみよう.

2 数と図形

最近 (2010 年),『ちくま学芸文庫』に 再録されたラーデマッヘル・テプリッツ著, 山崎三郎訳『数と図形』は実に興味深い本である. 私はこの本を高校 1 年生の頃先生から勧められた.

先生は,「訳文もいい.『何々するところの』というような表現はなくとてもこなれている」とおっしゃった. そこで放課後すぐに古本屋に行ったら幸いなことに買うことが出来た. そしてこの本に導かれて私は数学の深みにはまって行った. 今から振り返ると驚くほどの幸運に恵まれ数学者に仲間入りできた. 実に不思議なことである.

この本の 19 章で循環小数が扱われており, 私は小数展開の持つ魅力に引きつけられた. 最後に, 分母が素数の場合, その 2 分割和に 9 が並ぶことの証明が載っていたが, 高校生の私には十分理解できなかった. 次にその証明のアイデアを紹介しよう.

$\frac{a}{b}$ は既約分数で 10 進展開するとき, 長さ n で純循環するとしよう.

循環節を $a_1a_2\cdots a_n$ と書くときそれは $g=10$ とおけば $a_1g^{n-1}+a_2g^{n-2}+\cdots+a_n$ を表す. これを記号で $\langle a_1,a_2,\cdots,a_n\rangle_g$ と表す. $M=\langle a_1,a_2,\cdots,a_n\rangle_g$ とおくとき

$$\begin{aligned}\frac{a}{b}&=0.a_1a_2\cdots a_na_1a_2\cdots a_n\cdots\\&=\frac{a_1}{g}+\frac{a_2}{g^2}+\cdots+\frac{a_n}{g^n}+\frac{a_1}{g^{n+1}}\cdots+\frac{a_{2n}}{g^{2n}}+\cdots\\&=\frac{M}{g^n}+\frac{M}{g^{2n}}\cdots\\&=\frac{M}{g^n}(1+g^{-n}+g^{-2n}+\cdots)\\&=\frac{M}{g^n}\frac{1}{1-g^{-n}}\\&=\frac{M}{g^n-1}.\end{aligned}$$

結局

$$\frac{M}{g^n-1}=\frac{a}{b}\tag{1}$$

が得られ, これが分数と循環節の関係を表している. 分母を払うと $bM=a(g^n-1)$ になるので b を法として合同式で書けば

$$a(g^n-1)\equiv 0 \mod b.$$

a,b は互いに素なのでユークリッドの補題を使うと 整数 s,t があり $1=as+bt$ を満たす. よって $as\equiv 1 \mod b$. そこで s を掛ければ $as(g^n-1)\equiv g^n-1\equiv 0 \mod b$.

これより

$$g^n\equiv 1 \mod b.\tag{2}$$

よって $g^n-1=bD$ と整数 D で表せる. $bM=a(g^n-1)=abD$ により, $M=aD$. したがって $L=g^n-1$ とおくと D は M と L の公約数である.

a,b は互いに素なので D は M と L の最大公約数になる.

2.1 例

$\frac{3}{7}$ の循環節は 4 2 8 5 7 1 なので $M=428571, L=10^6-1=999999$ とおくと最大公約数 GCD $(M,L)=142857$ となる.

循環節の長さ n は $g^n\equiv 1 \mod b$ を満たす最小の正の整数なのである.(このことは後に示す)

2.2 長さが偶数のとき

b が素数 p で n が偶数 $2w$ のとき

$$\frac{M}{g^{2w}-1}=\frac{a}{p}$$

なので $pM=a(g^n-1)$. よって,

$$a(g^{2w}-1)\equiv a(g^n-1)\equiv 0 \mod p$$

を満たす.

a と p とは互いに素なのでユークリッドの補題を使えば $g^n-1\equiv 0 \mod p$ が導かれる.

$$(g^w-1)(g^w+1)=g^{2w}-1\equiv 0 \mod p \tag{3}$$

を得る. 一方 $g^w-1\neq 0$ なので $g^w+1\equiv 0$ をえる. すなわち $g^w+1=kp$ と書ける.

$pM=a(g^w-1)(g^w+1)=akp(g^w-1)$ より $M=ak(g^w-1)$.

$L=g^w-1$ とおくと $M=akL$.

循環節 M に対してその 2 分割の

前半の数を A, 後半の数を B とおけば $M=Ag^w+B$. かつ $A\leq L, B\leq L$ により $A+B\leq 2L$.

よって $M=Ag^w+B=A(g^w-1)+A+B=AL+A+B$ なので

$AL+A+B=akL$ を整理すると

$$A+B=akL-AL=(ak-A)L.$$

$d=ak-A$ とおけば

$$(ak-A)L=dL=A+B\leq 2L.$$

よって $0<d\leq 2$ により $d=1$ または $d=2$.

ここで $d=2$ とすると $A=L, B=L$ になる. そこで

$$M=Ag^w+B=A(g^w+1)=L(g^w+1)=g^{2w}-1$$

によれば

$$\frac{a}{p}=\frac{M}{g^{2w}-1}=\frac{M}{M}=1$$

となり矛盾. したがって,$d=1$. よって

$$A+B=L=g^w-1.$$

$g=10$ のときは $g^w-1=999\cdots 9$.

したがって循環節 M の前半の数 A, 後半の数 B の和 $A+B$ が $g^w-1=999\cdots 9$ となることが示された.

3 長さが 3 の倍数の時

以上の議論を長さが 3 の倍数の時, すなわち $n=3w$ の場合に適用してみよう. これは新しい見方である.

$L = g^w - 1$ を再び使う.

$$pM = a(g^{3w} - 1) = a(g^w - 1)(g^{2w} + g^w + 1) = aL(g^{2w} + g^w + 1)$$

$$g^{3w} - 1 = g^n - 1 \equiv 0 \mod p$$

を満たすが $g^w - 1 \not\equiv 0$ なので $g^{2w} + g^w + 1 \equiv 0$ をえる. すなわち $g^{2w} + g^w + 1 = cp$ と整数 c で書ける.

$pM = a(g^{3w} - 1) = a(g^w - 1)(g^{2w} + g^w + 1) = acp(g^w - 1) = apcL$ より $M = acL$.

循環節 M に対してその前 1/3 の数 A, 中 1/3 の数 B, 後 1/3 の数 C とおけば $M = Ag^{2w} + Bg^w + C$.

$L = g^w - 1$ によって $g^w = L + 1$ を代入すると

$$\begin{aligned} M &= Ag^{2w} + Bg^w + C \\ &= A(L+1)^2 + B(L+1) + C \\ &= L(AL + 2A + B) + A + B + C. \end{aligned}$$

よって $M = A + B + C + L(2A + AL + B)$ になり $M = acL$ を思い出せば,

$A + B + C + L(2A + AL + B) = acL$ を整理すると

$$A + B + C = L(ac - 2A - AL - B).$$

$d = ac - 2A - AL - B$ とおけば $A + B + C = dL$.

$A \le L = g^w - 1, B \le L, B \le L$ によって

$$dL = A + B + C \le 3L.$$

$0 < d \le 3$ により , $d = 1, 2, 3$.

ここで $d = 3$ とすると $A = B = C = L$ になり

$$M = Ag^{2w} + Bg^w + C = A(g^{2w} + g^w + 1) = L(g^{2w} + g^w + 1) = g^{3w} - 1.$$

よって

$$\frac{a}{p} = \frac{M}{g^{3w} - 1} = \frac{M}{M} = 1$$

となり矛盾. したがって,$d = 1, 2$ となる. よって

$$A + B + C = g^w - 1, \text{ または } 2(g^w - 1).$$

$A + B + C$ は循環節の 3 分割和だから, L(10 進なら 9 が並ぶ) または $2L$.

例

$\frac{7}{13}$ の循環節は $M = 538461$ なので $n = 6, w = 2$. $A = 53, B = 84, C = 61$ により $L = 99$, $A + B + C = 53 + 86 + 61 = 198 = 2 \times 99$.

4　最小性の証明

2.1 において，循環節の長さ n は $g^n \equiv 1 \mod b$ を満たす最小の正の整数である, と述べたがこの証明は意外にも難しい.

循環節の長さ n は $g^n \equiv 1 \mod b$ を満たすことは良い. しかし, $g^n \equiv 1 \mod b$ を満たす最小の正の整数 n が循環節の長さと言って良いかどうかという疑問が残る. そこで,

$g^m \equiv 1 \mod b$ を満たす最小の正の整数 m をとりこれを m で示す.

循環節の長さ n に対して $n \geq m$ を満たす.

n を m で割った商を s 余りを r とおく.

$$n = sm + r.$$

そこで指数の計算を次のように行う.

$$g^n \equiv 1, g^n = g^{ms+r} = (g^m)^s g^r \equiv g^r \mod b.$$

よって

$$1 \equiv g^r \mod b.$$

これは $r < m$ によれば m の最小性に反する. したがって $n = ms$ となる. $L = g^n - 1$, $D = \gcd(M, L)$ とおくと $M = aD, L = bD$ となる.

$$bD = L = g^n - 1 = g^{ms} - 1$$

に注意して $h = g^m$ とおけば 等比数列の和の公式を用いて

$$g^{ms} - 1 = h^s - 1 = (h-1)(h^{s-1} + h^{s-2} + \cdots + h + 1)$$

と変形する. $K = h^{s-1} + h^{s-2} + \cdots + h + 1$, とおき $g^m \equiv 1 \mod b$ に注意して $g^m - 1 = bD_1$ とおく.

$L = bD = (g^m - 1)K = bD_1K$ より $D = D_1K$. $M = aD = aD_1K$ なので $M_1 = aD_1$ とおけば

$$M = aD_1K = M_1K = M_1(h^{s-1} + h^{s-2} + \cdots + h + 1).$$

$a < b$ によって $M_1 = aD_1 < bD_1 = L_1$.

ここで $L_1 = g^m - 1$.

$$M = aD_1K = M_1K = M_1(g^{m(s-1)} + g^{m(s-2)} + \cdots + g^m + 1).$$

そこで

$$M = M_1(g^{m(s-1)} + \cdots + g^m + 1) = M_1g^{m(s-1)} + \cdots + M_1g^m + M_1$$

は循環節 M が M_1 を s 個並べたものになっている．M_1 を M として選んでおけば良い.

お断り

循環小数の性質を詳しく調べるには, ここで述べた方法は実力不足である. 本格的に研究するには, ガウスの展開した数の合同の考えを使うのが良い．今回は, 循環小数の性質のいろいろな性質を見せ, 証明を手軽に述べることを優先した. 先進的な読者は今月号の論法に物足りなさを覚えたであろう. 夏休み明けの頃にはもっと本格的な循環小数の研究を紹介する予定である.

5　付録:ユークリッドの補題

補題 1 自然数 a,b に対してその最大公約数を d とおくと整数 s,t があり $d=as+bt$ と書ける.

これを**ユークリッドの補題**という.

平成 24 年度から施行されている高校の学習指導要領では数学 A で整数の性質が取り上げられている. 自然数 a,b の最大公約数を求めるためにユークリッドの**互除法**が扱われている.

互除法とはその名の通りで, 互いに割って行くとついに最大公約数になるというものである.

- a を b で割った余りを r_1 とおく.
- b を r_1 で割った余りを r_2 とおく.
- r_1 を r_2 で割った余りを r_3 とおく.
- $b>r_1>r_2>\cdots$ となるのでいつかは $r_j=0$ になる.

0 になる 1 つ前の余り r_{j-1} が 最大公約数である. 互除法の例を示そう.

$a=486, b=189$ とするとき次の図式を最初に書く.

表 5: 最初の図式

1	0	489
0	1	189

- 486 を 189 で割った商 2 を 2 行目の左に書く.
- 3 次の行ベクトル $\overrightarrow{v_1}=(1,0,489), \overrightarrow{v_2}=(0,1,189)$ とおきベクトル $\overrightarrow{v_1}-2\overrightarrow{v_2}=(1,-2,108)$ を第 2 行の 2 項に書く.
- 189 を 108 で割った商 1 を 3 行目の左に書く.
- ベクトルの計算を続ける.
- 81 を 27 で割ると割り切れたので,27 が最大公約数.
- 5 行目の 2 項からのベクトル $(2,-5,27)$ の第 1,2 成分を s,t とおくと $as+bt=27$.
- 6 行目の 2 項からのベクトル $(-7,18,0)$ の第 1,2 成分を x,y とおくと $ax+by=0$.

5.1　イデアルによる証明

ユークリッドの補題を本格的に証明しよう.

a,b を 0 でない自然数 (整数でも成立する) とし集合 $J=\{ak+bl \mid k,l\in\mathbb{Z}\}$ を定義すると, 次の性質を持つ.

- $n,m\in J$ なら $n+m\in J$,

表 6: 計算の終わった図式

	1	0	489
2	0	1	189
1	1	-2	108
1	-1	3	81
3	2	-5	27
	-7	18	0

- $x \in \mathbb{Z}, n \in J$ なら $xn \in J$.

このような性質をもつ集合を一般にイデアルという.
$J \neq \{0\}$ なので J に属する自然数の中での最小数を δ とする.
J の元 c は必ず δ の倍数になることを以下で示そう.
$c > 0$ と仮定しても一般性を失わない. これを δ で割り, その商を q, 余りを r とおく. すると

$$c = q\delta + r, \quad (0 \leq r < \delta)$$

を満たす. そこで 集合 J の性質により $r = c + (-q)\delta \in J$. $r < \delta$ かつ, δ は J に属する自然数の中で最小だったから, $r = 0$. よって $c = q\delta$. すなわち c は δ の倍数.

一方 a, b は J の元なので, 上で示したことによるとこれらは δ の倍数になり, δ は a, b の公約数である.

さて $\delta \in J$ なので整数 s, t により $\delta = as + bt$ と書ける. ところで, a, b の正の公約数 d をとると $a = da_0, b = db_0$ と整数 a_0, b_0 で書けるから,

$$\delta = as + bt = d(a_0 s + b_0 t)$$

となるので, $\delta \geq d$. ゆえに δ は a, b の公約数の中で最大. すなわち最大公約数であることがわかった.

5.2 数学 A

某社の数学 A の教科書には, 第 2 章整数の性質, において 2 元 1 次不定方程式が扱われ次の性質が証明無しで述べられている.

性質 1 整数 a, b が互いに素で, 整数 x, y があって $ax = by$ を満たすなら y は a の倍数, x は b の倍数となる.

この証明はユークリッドの補題を使えば簡単である.
a, b の最大公約数は 1 なので $as + bt = 1$ を満たす整数があり, これに x を掛けると

$$asx + btx = x,$$

$asx = sby$ により

$$x = asx + btx = sby + btx = b(sy + tx).$$

$f = sy + tx$ とおけば, $x = bf, y = af$.

この性質は使いやすいが, 次の形で述べられることが多い.

性質 2 整数 a,b は互いに素とする. ax が b の倍数なら x は b の倍数となる.

b が素数 p のとき次の結果になる.

性質 3 p が ac の素因子なら, a または x の素因子になる.

このことは自然数において素因数分解が一意的なことを意味する. 逆に素因数分解が一意的なことを認めれば, 性質 3 も性質 1 もすぐ示される.

高校までの教育では自然数において素因数分解が一意的なことは証明されていないが自明のこととして扱われることがある. すると, 性質 1 も当然の事実となる. ユークリッドの補題はきわめて大切な結果で, これによって初めて素因数分解が一意的なことが証明され, そのときのキーが性質 1 なのである.

参考文献

ラーデマヘル・テプリッツ著, 山崎三郎, 鹿野健訳『数と図形』, ちくま学芸文庫 (筑摩書房, 2010)
飯高 茂 著 『環論, これはおもしろい』(数学のかんどころ, 共立出版, 2013)