循環小数の２分割和の研究

浅野史織
西原浩子
学習院大学理学部数学科

平成 20 年 2 月 2 日

目 次

1　目的

　はじめに次のような例について考える.

$\frac{1}{7} = 0.\dot{1}4285\dot{7}$

このように $\frac{1}{7}$ を 10 進展開した循環節を半分に分けて足すと

142 + 857 = 999 となる.

　一般に，奇素数 p について $\frac{1}{p^r}$ の循環節の長さが偶数の時，循環節を半分に分けて加えると，g が並ぶことはよく知られている.

この研究においては，200 以下の自然数 N を分母とし、$\frac{1}{N}$ を小数に３進展開したときの循環節の長さが偶数 $2m$ のとき、循環節をリストで $[q_1, q_2, \cdots, q_{2m}]$ と表示する。それを $[q_1, q_2, \cdots, q_m], [q_{m+1}, q_{m+2}, \cdots, q_{2m}]$ のように２分割する。

これらについて桁上がりも考えて対応する成分を加えてできた数（これを分割和という）について，同じような性質がいつ成り立つか研究を行う。

　素数は 2 と奇素数に分けられる。この研究では、素数の中で特別な存在である 2 について詳しく知ることを目的とし、３進展開を扱った。

　特に、この２分割和が $[2, 2, \cdots, 2]$ の形で表される自然数 N の性質が以下の 4 通りである場合について調べる。

1. $N = p^k$ (p は奇素数) のとき
2. $N = 4$ のとき
3. $N = 2 \times p^k$ (p は素数) のとき
4. $N = 4 \times p^k$ ($p \equiv 7$ mod 12) のとき

2　方法

%%%%%　プログラム　%%%%%

```
/* for */
for(I=<J,I) :- I =<J.
for(I=<J,K) :- I =<J,
   I1 is I+1,for(I1 =<J,K).


/* 因数分解 */
factor(P/2):-Q is P//2,P =:= 2*Q,!.
factor(P/I):-P1 is floor(sqrt(P)),
```

```
   for(1 =< P1,J),
      J1 is 2*J+1,
   Q is P//J1,
      P =:= J1*Q,I= J1,!.
factor(P/P) :-!.

factorize(P,[P]):- factor(P/Q),Q==P,!.
factorize(P,List):- factor(P/I),
      P1 is P//I,
      List=[I|List1],
      factorize(P1,List1),!.




/** 最大公約数 **/
gcd(A=(A,0)):-!.
gcd(D=(A,B)):-B1 is A mod B,A1=B,
              gcd(D=(A1,B1)).


/** 商とあまり **/
res_q(A=B*Q+R) :- Q is A//B,R is A-B*Q.




/** リストの結合と分解 append0/1 の定義 **/
append0(Z = [] + Z).
append0([A|Z] = [A|X] + Y) :- append0(Z = X +Y).


/** リストを２分割 **/
left(A=[]+A,0) :- !.
left(A=B+C,N) :- N>0,N1 is N-1,!,
    left(A=B1+[X|C],N1) , append0(B=B1+[X]),!.

half(L=A+B) :- length(L,N),N1 is N/2,
               left(L=A+B,N1).


/** 10 進数を G 進数で表し、リストで表記する **/
dig_g(N,[N],G) :- N<G.
dig_g(N,L,G) :- N1 is N//G,
                R1 is N mod G,
```

```
      dig_g(N1,L1,G),
      append0(L=L1+[R1]).

g_dig(N,[N],G) :- N<G,
g_dig(X,L,G) :- append0(L = N + [R]),
                g_dig(Y,N,G),
                X is Y * G + R.
```

```
/* ２分割和 */
gdig(A=B+C,G):- g_dig(X,B,G),
                g_dig(Y,C,G),
                Z is X+Y,
dig_g(Z,A,G),!.
```

```
/** 1/B の G 進数小数展開における商のリストと長さ **/

junku4(B,G,L,SS) :-1<B,
junku4_aux([1/B,G],1,0,[],L),length(L,SS),
                   %    write(SS),
                        !.
junku4_aux([1/B,G],1,R,L,L) :-R>0,!.
junku4_aux(Const,A,R,W,L) :-Const = [1/B,G],
                             A1 is A*G,
                             res_q(A1=B*Q+R1),
                          %   write(Q),tab(1),
                             append0(W1=W+[Q]),
                             junku4_aux(Const,R1,R1,W1,L).
```

```
/** B=A～C のとき,1/B の G 進数循環節の長さが偶数のときの２分割和 **/

ninoichi(B,G,P) :- junku4(B,G,L,SS),
      gcd(D1=(2,SS)),
      (D1==2 -> half(L=X+Y),
% write(L),
gdig(P=X+Y,G)).
```

```
ninoichi2(A,C,G):- for(A=<C,B),
gcd(D1=(B,G)),
D1==1,
ninoichi(B,G,P),nl,
factorize(B,L),write(L),tab(3),
write(1/B),
write('='),
write(P),nl,fail.
ninoichi2(A,C,G).


/** 表を作成する **/
hyo(A,C,G) :- for(A=<C,B),
                (gcd(D1=(B,G)),D1==1,
                nl,
write(B),tab(2),
factorize(B,N),write(N),tab(3),
junku2(B,G,L),write(L),tab(3),
ninoichi(B,G,Q),write(Q),tab(3),
ninoni1(B,G,P),write(P),tab(3)),fail.
hyo(A,C,G).
```

3　結果

N = 1〜200 のとき $\frac{1}{N}$ の 3 進展開の 2 分割和が [2,2,$\cdots$,2](2 が並ぶ) となる自然数 N について、表 1 にまとめる。

表 1: 全部の結果

N の値	因数分解	2 分割和	2 が並ぶ個数
4	[2, 2]	[2]	1
5	[5]	[2, 2]	2
7	[7]	[2, 2, 2]	3
10	[2, 5]	[2, 2]	2
14	[2, 7]	[2, 2, 2]	3
17	[17]	[2, 2, $\cdots$, 2, 2]	8
19	[19]	[2, 2, $\cdots$, 2, 2]	9
25	[5, 5]	[2, 2, $\cdots$, 2, 2]	10
28	[2, 2, 7]	[2, 2, 2]	3
29	[29]	[2, 2, $\cdots$, 2, 2]	14
31	[31]	[2, 2, $\cdots$, 2, 2]	15
34	[2, 17]	[2, 2, $\cdots$, 2, 2]	8
37	[37]	[2, 2, $\cdots$, 2, 2]	9
38	[2, 19]	[2, 2, $\cdots$, 2, 2]	9
40	[2, 2, 2, 5]	[2]	1
41	[41]	[2, 2, 2, 2]	4
43	[43]	[2, 2, $\cdots$, 2, 2]	21
49	[7, 7]	[2, 2, $\cdots$, 2, 2]	21
50	[2, 5, 5]	[2, 2, $\cdots$, 2, 2]	10
53	[53]	[2, 2, $\cdots$, 2, 2]	26
58	[2, 29]	[2, 2, $\cdots$, 2, 2]	14
61	[61]	[2, 2, 2, 2, 2]	5
62	[2, 31]	[2, 2, $\cdots$, 2, 2]	15
67	[67]	[2, 2, $\cdots$, 2, 2]	11
73	[73]	[2, 2, 2, 2, 2, 2]	6
74	[2, 37]	[2, 2, $\cdots$, 2, 2]	9
76	[2, 2, 19]	[2, 2, $\cdots$, 2, 2]	9
79	[79]	[2, 2, $\cdots$, 2, 2]	39
82	[2, 41]	[2, 2, 2, 2]	4
86	[2, 43]	[2, 2, $\cdots$, 2, 2]	21
89	[89]	[2, 2, $\cdots$, 2, 2]	44
91	[7, 13]	[2, 2]	2
97	[97]	[2, 2, $\cdots$, 2, 2]	24
98	[2, 7, 7]	[2, 2, $\cdots$, 2, 2]	21
101	[101]	[2, 2, $\cdots$, 2, 2]	50
103	[103]	[2, 2, $\cdots$, 2, 2]	18
106	[2, 53]	[2, 2, $\cdots$, 2, 2]	26
113	[113]	[2, 2, $\cdots$, 2, 2]	56
122	[2, 61]	[2, 2, 2, 2, 2]	5
124	[2, 2, 31]	[2, 2, $\cdots$, 2, 2]	15
125	[5, 5, 5]	[2, 2, $\cdots$, 2, 2]	50
127	[127]	[2, 2, $\cdots$, 2, 2]	63
133	[7, 19]	[2, 2, $\cdots$, 2, 2]	9
134	[2, 67]	[2, 2, $\cdots$, 2, 2]	11
137	[137]	[2, 2, $\cdots$, 2, 2]	68
139	[139]	[2, 2, $\cdots$, 2, 2]	69
145	[5, 29]	[2, 2, $\cdots$, 2, 2]	14
146	[2, 73]	[2, 2, $\cdots$, 2, 2]	6
148	[2, 2, 37]	[2, 2, $\cdots$, 2, 2]	9
149	[149]	[2, 2, $\cdots$, 2, 2]	74
151	[151]	[2, 2, $\cdots$, 2, 2]	25
157	[157]	[2, 2, $\cdots$, 2, 2]	39
158	[2, 79]	[2, 2, $\cdots$, 2, 2]	39
163	[163]	[2, 2, $\cdots$, 2, 2]	81
172	[2, 2, 43]	[2, 2, $\cdots$, 2, 2]	21
173	[173]	[2, 2, $\cdots$, 2, 2]	86
178	[2, 89]	[2, 2, $\cdots$, 2, 2]	44
193	[193]	[2, 2, $\cdots$, 2, 2]	8
194	[2, 97]	[2, 2, $\cdots$, 2, 2]	23
196	[2, 2, 7, 7]	[2, 2, $\cdots$, 2, 2]	21
197	[197]	[2, 2, $\cdots$, 2, 2]	98
199	[199]	[2, 2, $\cdots$, 2, 2]	99

表 1 の結果をもとに、因数分解のリストに注目し以下 5 つの性質ごとに表 2〜6 にまとめる。

表 2: $N = p^k$(p は奇素数)

N の値	因数分解		N の値	因数分解
5	[5]		97	[97]
7	[7]		101	[101]
17	[17]		103	[103]
19	[19]		113	[113]
25	[5, 5]		125	[5, 5, 5]
29	[29]		127	[127]
31	[31]		137	[137]
37	[37]		139	[139]
41	[41]		149	[149]
43	[43]		151	[151]
49	[7, 7]		157	[157]
53	[53]		163	[163]
61	[61]		173	[173]
67	[67]		193	[193]
73	[73]		197	[197]
79	[79]		199	[199]
89	[89]			

表 3: $N = 4$

N の値	因数分解
4	[2, 2]

表 4: $N = 2p^k$

N の値	因数分解		N の値	因数分解
10	[2, 5]		86	[2, 43]
14	[2, 7]		98	[2, 7, 7]
34	[2, 17]		106	[2, 53]
38	[2, 19]		122	[2, 61]
50	[2, 5, 5]		134	[2, 67]
58	[2, 29]		146	[2, 73]
62	[2, 31]		158	[2, 79]
74	[2, 37]		178	[2, 89]
82	[2, 41]		194	[2, 97]

表 5: $N = 4p^k$

N の値	因数分解
28	[2, 2, 7]
76	[2, 2, 19]
124	[2, 2, 31]
172	[2, 2, 43]
196	[2, 2, 7, 7]

表 6: その他

N の値	因数分解
40	[2, 2, 2, 5]
91	[7, 13]
133	[7, 19]
145	[5, 29]
148	[2, 2, 37]

4　一般的な理論

既約の真分数 $\frac{a}{b}$ を小数に 3 進展開することを考える．ただし，3 と b は互いに素で，a と b も互いに素とする．$a < b$ なので $3 \times a$ を考え，これを b で割ると

$$3a = q_1 b + r_1$$

さらに $3r_1$ を b で割ると

$$3r_1 = q_2 b + r_2$$

これを繰り返す．ただし，$j = 2, 3, \cdots$ について

$$\begin{aligned} 3r_2 &= q_3 b + r_3, \\ &\vdots \\ 3r_{j-1} &= q_j b + r_j, \\ 3r_j &= q_{j+1} b + r_{j+1}. \end{aligned}$$

b を法として考えると，

$$\begin{aligned} 3a &\equiv r_1 \bmod b, \\ 3r_1 &\equiv r_2 \bmod b, \\ &\vdots \\ 3r_{j-1} &\equiv r_j \bmod b. \end{aligned}$$

上記のものを並べ替えると，

$$\begin{aligned} r_j &\equiv 3r_{j-1} \bmod b, \\ &\vdots \\ r_2 &\equiv r_1 \bmod b, \\ r_1 &\equiv 3a \bmod b. \end{aligned}$$

よって，

$$r_j \equiv 3^j a \bmod b.$$

r_j が公比 3 の等比数列となった．

$r_j \equiv r_k \bmod b$ なら $g^j a \equiv g^k a \bmod b$ により，

$$(g^j - g^k)a \equiv 0 \bmod b.$$

a，b は互いに素なので,$a \bmod b$ は逆元をもち，

$$3^j \equiv 3^k \bmod b.$$

3 と b は互いに素なので，$3 \bmod b$ は逆元をもち，

$$3^{j-k} \equiv 1 \bmod b.$$

を満たす．そこで u を $g \bmod b$ の乗法群の元としての位数（$ord_b(g)$ とも書く）とすれば，

$$j - k \equiv 0 \bmod u$$

を得る．これは，次の補題より導かれる．

$\boxed{\text{補題}}$ u を 3 での mod$b$ の位数.$3^A \equiv 1 \bmod b$ なら A は u の倍数

証明
A を u で割って，商を Q，余りを R とすると，$A = uQ + R$ となり

$$3^A \equiv 3^{uQ+R}$$
$$3^A \equiv 3^{uQ} \times 3^R.$$

$3^u \equiv 1$ より

$$1 \equiv 1 \times 3^R,$$
$$3^R \equiv 1.$$

$0 < R < u$ なので $R = 0$．よって $A = uQ$.

[終]

今まで結果を定理 4.1 にまとめる.

$\boxed{\text{定理 4.1}}$

$$r_j \equiv 3^j a \bmod b,$$
$$r_j = r_k \Longleftrightarrow j \equiv k \bmod u.$$

$u = ord_b(3)$ とする.
3 の位数 (周期）u が合成数 ms とする.
等比級数の和の公式と同じように

$$(1 - 3^m)(1 + 3^m + \cdots + 3^{m(s-1)}) = 1 - 3^{ms} = 1 - 3^u \equiv 0 \bmod b.$$

mod$b$ において $1 - 3^m$ が逆元をもてば（すなわち $1 - 3^m$ が b と互いに素なら)

$$1 + 3^m + \cdots + 3^{m(s-1)} \equiv 0 \bmod b.$$

以下，$s = 2$ について考えてみる.

《s = 2 の場合》

$$3^{2m} \equiv 1 \bmod b$$

$x \equiv 3^m \bmod b$ とおくと，

$$x^2 \equiv 1 \bmod b.$$

b を法としたときの合同数の環を Z/bZ と書くとき，その乗法群 $U(Z/bZ)$ が巡回群なら $x = -1 \bmod b$.
$b = p^k, 4, 2p^k$（p は奇素数）の場合，乗法群 $U(Z/bZ)$ は巡回群になることが知られている．今回は $3^m \equiv -1 \bmod b$. よって，

$$r_{j+m} \equiv 3^{j+m}a \equiv 3^m 3^j a \equiv -r_j \bmod b.$$

これより

$$r_{j+m} \equiv -r_j \bmod b,$$
$$r_{j+m} + r_j \equiv 0 \bmod b.$$

$0 < r_{j+m}, r_j < b$ より

$$r_{j+m} + r_j = b.$$

一方，

$$3r_j = q_{j+1}b + r_{j+1}, \cdots (1)$$
$$3r_{j+m} = q_{j+1+m}b + r_{j+1+m}. \cdots (2)$$

(1),(2) を加えて，

$$3(r_j + r_{j+m}) = (q_{j+1} + q_{j+m+1})b + r_{j+1} + r_{j+m+1},$$
$$3b = (q_{j+1} + q_{j+m+1})b + b,$$
$$3 = q_{j+1} + q_{j+m+1} + 1,$$
$$3 - 1 = q_{j+1} + q_{j+m+1},$$
$$2 = q_j + q_{j+m}. \ (j + 1 = j \text{ とおく})$$

まとめて次の結果を得られる．

$\boxed{\text{定理 4.2}}$ $b = p^k, 4, 2p^k$ (p は奇素数),3 の $U(Z/bZ)$ での位数 (周期) が偶数 $2m$ なら循環節を半分にして各数を足す (2 分割和) とみな 2 になる．

5　考察

因数分解の結果に着目し、以下の４つのパターンに分けて考察する。

5.1　一般的理論から

5.1.1　$N = p^k$ (p は奇素数) のとき

表 2 参照により $N = p^k$ (p は奇素数) のとき 2 分割和が [2,2,$\cdots$,2](2 が並ぶ) となることがわかる。

5.1.2　$N = 4$ のとき

表 3 参照により $N = 4$ のとき 2 分割和が [2,2] となることがわかる。

5.1.3　$N = 2 \times p^k$ (p は素数) のとき

表 4 参照により $N = 2 \times p^k$ (p は素数) のとき 2 分割和が [2,2,$\cdots$,2](2 が並ぶ) となることがわかる。

5.1.1～5.1.3 は、前節の一般的理論から導き出された定理 4.2 により証明することができた。
次に、この研究を通して上記の定理 4.2 で述べられていない N の性質について 5.2 で証明する。

5.2　N $= 4 \times$ p^k (p $\equiv 7$ mod 12) のとき

表 5 参照により $N = 4 \times p^k$ ($p \equiv 7$ mod 12) のとき 2 分割和が [2,2,$\cdots$,2](2 が並ぶ) となることがわかる ($N \leq 200$) 。

$u = 2m$ のとき,
$x \equiv 3^m$ mod $4p$ とおく.
$x^2 \equiv 3^{2m} \equiv 1$ mod $4p$ となる.

$\boxed{\text{このとき } x = -1 \text{ となることを証明する.}}$

<u>証明</u>

$$\begin{cases} ① \ 3^m \equiv x \bmod p \\ ② \ 3^m \equiv x \bmod 4 \end{cases}$$

＜①の場合＞

$$3^{2m} \equiv x^2 = 1 \bmod p$$
$$(x+1)(x-1) \equiv 0 \bmod p$$

<u>$x - 1 \not\equiv 0$ なら</u>

p は $(x-1)$ で割れないから，p と $(x-1)$ は互いに素.
$1 = \alpha p + \beta(x-1)$ となる整数 α,β がある.
$$1 \equiv \beta(x-1) \bmod p$$
$$\beta(x+1)(x-1) \equiv 0 \bmod p$$
$$x + 1 \equiv 0 \bmod p,$$
$$x \equiv -1.$$

<u>$x - 1 \equiv 0$ なら</u>

$$x \equiv 1 \bmod p,$$
$$\therefore x \equiv \pm 1 \bmod p.$$

＜②の場合＞

$$3 \equiv -1 \bmod 4$$

<u>m が奇数のとき,</u>

$$3^m \equiv (-1)^m \equiv -1 \bmod 4$$
$$x \equiv -1 \bmod 4$$

<u>m が偶数のとき,</u>

$$3^m \equiv (-1)^m \equiv 1 \bmod 4$$
$$3^m \equiv \pm 1 \bmod p \text{ より,}$$

・$3^m \equiv 1 \bmod p$ のとき,

$$(3^m \equiv 1 \bmod 4)$$
$$3^m \equiv 1 \bmod 4p$$

・$3^m \equiv -1 \bmod p$ のとき,

$$m = 2k,$$
$$3^k = X,$$
$$3^m = 3^{2k} = X^2 \equiv -1 \bmod p,$$
$$\left(\frac{-1}{p}\right) \equiv 1 \text{ のとき}, p \equiv 1 \bmod 4,$$

これは，$*$の p の条件 ($p \equiv 7 \bmod 12$) に反しているため矛盾.

定理 4.3
$X^2 \equiv -1 \bmod p$ となる解があるとき,$p \equiv 1 \bmod 4$

定義:平方剰余
$x^2 \equiv \alpha \bmod p$ に解があるとき
$\left(\frac{\alpha}{p}\right) = 1$
$x^2 \equiv \beta \bmod p$ に解がないとき
$\left(\frac{\beta}{p}\right) = -1$

以下，m が奇数の場合について考える.

$$\begin{cases} x \equiv \pm 1 \bmod p \cdots (1) \\ x \equiv -1 \bmod 4 \cdots (2) \end{cases}$$

(1) と (2) を合わせて,

<u>・$x \equiv 1 \bmod p$ のとき,</u>

$m = 2k + 1$(奇数だから)

$3^{2k} \times 3 \equiv 1 \bmod p$

ルジャンドルの記号
$(\frac{\alpha\beta}{p}) = (\frac{\alpha}{p})(\frac{\beta}{p})$

より，
平方剰余の定義を用いると，

$1 = (\frac{1}{p}) \equiv (\frac{3 \cdot 3^{2k}}{p})$
$\equiv (\frac{3}{p})(\frac{3^k}{p})^2 \quad ((\frac{3^k}{p})^2 = 1)$
$1 = (\frac{3}{p})$

相互法則
$(\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

より，

$(\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{p-1}{2}}$
$(1 = (\frac{3}{p}))$
$(\frac{p}{3}) = (-1)^{\frac{p-1}{2}}$

ここで，$p = 12\alpha + 7$ より $p \equiv 3 \bmod 4$.

$p = 3 + 4l$
$(\frac{p}{3}) = (-1)^{\frac{2-4l}{2}}$
$= (-1)^{1+2l}$
$= -1$
$\therefore (\frac{p}{3}) = (-1)$

ここで，一般的に $(\frac{a}{3}) = (-1)$ について考える.

$$\left(\begin{array}{c}
X^2 \equiv p \bmod 3 \\
a = 1 \text{ のとき} \quad X^2 \equiv 1 \quad (\frac{1}{3}) = 1 \quad \text{解あり} \\
a = 2 \text{ のとき} \quad X^2 \equiv 2 \bmod 3 \text{ の解は,} \\
X = 1 \text{ のとき解なし} \\
X = 2 \text{ のとき解なし} \\
(\frac{2}{3}) = (-1) \Rightarrow p \equiv 2 \bmod 3 \\
\text{しかし}, p = 12\alpha + 7 \\
p \equiv 7 \bmod 3 \\
p \equiv 1 \bmod 3
\end{array}\right)$$

よって，$(\frac{a}{3}) = (-1)$ は矛盾.

・$x \equiv -1 \bmod p$ のとき，

$x \equiv -1 \bmod 4p$

以上より，$3^m \equiv x \bmod 4p$ で $x = -1$ となることが証明された.　　　[終]

6　今後の課題

今後の課題としては，以下のことが挙げられる．
２分割和が $[2, 2, \cdots, 2]$ の形で，表２～５に表れた自然数 N については証明できたが，表６（その他）に表れた自然数 N についての証明方法が未解決である．
また，３分割和がどのように表されるのか，３進展開以外にも８進展開や１０進展開でのそれぞれの分割和がどのようになるかについても検証する必要がある．

7　感想

◇浅野史織
プログラミングはわからないことばかりで，とっても大変でした．
しかし，飯高先生のご指導のおかげで，なんとか論文を書くことができてよかったです．
４年間ありがとうございました．

◇西原浩子
初めはプログラミングに対して抵抗があったのですが，少しずつ理解できるようになり楽しかったです．浅野さんと協力して無事に論文が書けて良かったです．又，飯高先生のゼミで本当に良かったと思います．有難うございました．