0.2　オイラー余関数の評価

素因数分解

$$a = p_1^{e_1} \cdots p_r^{e_r} = \prod_{j=1}^{r} p_j^{e_j}, (p_1 < \cdots < p_r)$$

に対して $\varepsilon(a) = \sum_{j=1}^{r} e_j$ とおく.

a の相異なる素因子の数を $s(a)$ と書く. したがって $s(a) = r$.

オイラー余関数は $co\varphi(a) = a - \varphi(a)$ によって定義される.

補題 1 $a > 1$ のとき a : 素数になる必要十分条件は $co\varphi(a) = 1$ である.

a が素数でないとき $co\varphi(a) \geq \sqrt{a}$ が成り立つ.
この証明は『数学の研究をはじめよう Ⅰ』に書かれている.
ここでは, $s(a) \geq 2$ に限ってこれらを $co\varphi(a)$ の順に並べた.
$s(a) = 1$ なら $a = p^e$ でそのときは $co\varphi(a) = p^{e-1}$

表 1: $co\varphi(a) - \sqrt{a}$; a が平方数でないとき,

a	factor	$\varphi(a)$	$co\varphi(a)$	$co\varphi(a) - \sqrt{a}$
6	$[2, 3]$	2	4	1.550510257
10	$[2, 5]$	4	6	2.83772234
15	$[3, 5]$	8	7	3.127016654
14	$[2, 7]$	6	8	4.258342613
12	$[2^2, 3]$	4	8	4.535898385
21	$[3, 7]$	12	9	4.417424305
35	$[5, 7]$	24	11	5.083920217
22	$[2, 11]$	10	12	7.30958424
20	$[2^2, 5]$	8	12	7.527864045
18	$[2, 3^2]$	6	12	7.757359313
33	$[3, 11]$	20	13	7.255437353

表 2: $co\varphi(a) - \sqrt{a}$

a	factor	$\varphi(a)$	$co\varphi(a)$	$co\varphi(a) - \sqrt{a}$
26	$[2, 13]$	12	14	8.900980486
55	$[5, 11]$	40	15	7.583801513
39	$[3, 13]$	24	15	8.755002002
28	$[2^2, 7]$	12	16	10.70849738
24	$[2^3, 3]$	8	16	11.10102051
77	$[7, 11]$	60	17	8.225035613
65	$[5, 13]$	48	17	8.937742252
34	$[2, 17]$	16	18	12.16904811
91	$[7, 13]$	72	19	9.460607986
51	$[3, 17]$	32	19	11.85857157
38	$[2, 19]$	18	20	13.835586
85	$[5, 17]$	64	21	11.78045554
57	$[3, 19]$	36	21	13.45016556
45	$[3^2, 5]$	24	21	14.29179607
30	$[2, 3, 5]$	8	22	16.52277442

命題 1 a が平方数でないとき, $co\varphi(a) - \sqrt{a} > 1.5$
さらに, $a \neq 6, 10, 15$ ならば $co\varphi(a) - \sqrt{a} > 4$

Proof.
$a = pq, (p < q : primes)$ のとき, 正の数 k を定め $co\varphi(a) - \sqrt{a} - k = p + q - 1 - \sqrt{pq} - k < 0$ とする.

$$p + q - 1 - \sqrt{pq} - k = \sqrt{q}(\sqrt{q} - \sqrt{p}) + p - k + 1 < 0$$

それゆえ

$$0 < \sqrt{q}(\sqrt{q} - \sqrt{p}) < k + 1 - p.$$

$0 < k_0 = k + 1 - p$ により $p < k + 1$.
$\alpha = \sqrt{q}$ とおくとき,

$$0 < \alpha^2 - \sqrt{p}\alpha < k_0.$$

根の公式により 判別式を D とおくと $D = p + 4k_0$.
2 次方程式 $t^2 - \sqrt{p}t - k_0 = 0$ の解は $\frac{\sqrt{p} \pm \sqrt{D}}{2}$
この大きいほうの 根を t_2 とおけば

$$t_2 = \frac{\sqrt{p} + \sqrt{D}}{2}.$$

さらに

$$q = \alpha^2 \geq {t_2}^2.$$

1.$k = 4$ のとき,
$p < k + 1 = 5$ なので, p は素数だから,$p = 2, 3$.
1a. $p = 3$. このとき, $k_0 = 2, D = p + 4k_0 = 3 + 8 = 11 < 12$.

$$t_2 = \frac{\sqrt{p} + \sqrt{D}}{2} < \frac{\sqrt{3} + \sqrt{12}}{2} = \frac{3\sqrt{3}}{2} = 2.6 \cdots .$$

ゆえに $q \geq {t_2}^2 = 6.75 \cdots$. ゆえに $q = 5$.
1b. $p = 2$. このとき, $k_0 = 3, D = p + 4k_0 = 14 < 16$.

$$t_2 = \frac{\sqrt{p} + \sqrt{D}}{2} < \frac{\sqrt{2} + \sqrt{16}}{2} = \frac{\sqrt{2} + 4}{2} = 2.7 \cdots .$$

ゆえに $q \geq 2.7^2 = 7.29 \cdots$. ゆえに $q \leq 7$. $p = 2 < q = 3, 5, 7$. しかし $p = 2, q = 7$ は不等式を満たさない.
$a = 6, 10, 15$ が解になる.

2.$k = 7$ のとき,

$p < k+1 = 8$ なので, p は素数だから,$p = 2, 3, 5, 7$.
同様の議論で, 解は次のとおり.
$6 = [2, 3]$, $10 = [2, 5]$, $15 = [3, 5]$, $14 = [2, 7]$ $12 = [2^2, 3]$ $21 = [3, 7]$.
また 3 次の評価式も出ている.
ここでは, $s(a) \geq 2$ に限ってこれらを $co\varphi(a)$ の順に並べた.

表 3: $\mathrm{co}\varphi(a) - a^{(2/3)}$

a	factor	$\varphi(a)$	$co\varphi(a)$	$\mathrm{co}\varphi(a) - a^{(2/3)}$
187	$[11, 17]$	160	27	-5.701002815
143	$[11, 13]$	120	23	-4.345803682
91	$[7, 13]$	72	19	-1.231477245
119	$[7, 17]$	96	23	-1.193459517
77	$[7, 11]$	60	17	-1.099246023
133	$[7, 19]$	108	25	-1.055600934
35	$[5, 7]$	24	11	0.300125194
55	$[5, 11]$	40	15	0.537552581
6	$[2, 3]$	2	4	0.698072751
65	$[5, 13]$	48	17	0.833764374
15	$[3, 5]$	8	7	0.917798004
10	$[2, 5]$	4	6	1.358411166
21	$[3, 7]$	12	9	1.388337389
85	$[5, 17]$	64	21	1.667888834
95	$[5, 19]$	72	23	2.17991954
14	$[2, 7]$	6	8	2.191214266
33	$[3, 11]$	20	13	2.711723522
12	$[2^2, 3]$	4	8	2.758517212
115	$[5, 23]$	88	27	3.351774378
39	$[3, 13]$	24	15	3.499684949
22	$[2, 11]$	10	12	4.148575589
20	$[2^2, 5]$	8	12	4.631937003
18	$[2, 3^2]$	6	12	5.131714545
26	$[2, 13]$	12	14	5.223617045
51	$[3, 17]$	32	19	5.247548646
57	$[3, 19]$	36	21	6.189039043

0.3　オイラー余関数の新しい評価式

長野県 飯山高校の生徒さんは次の形に一般化しオイラー余関数の新しい評価式をえた. このような評価式が成立することを私は予想すらしていなかった.

定理 1 (飯山高校) 自然数 $m > 1$ について次の評価式が成り立つ.
$\varepsilon(a) \geq m$ のとき

$$co\varphi(a) \geq a^{\frac{m-1}{m}}$$

とくに $m = 2$ なら,a が素数の平方でないなら $co\varphi(a) \geq \sqrt{a}$
$m = 3$ なら $a = pq$ の場合を除くと $co\varphi(a) \geq \sqrt[3]{a^2}$
Proof.
1. $r = 1$.
$e = e_1.p = p_1$ と書くとき $p^e, e \geq m$ なので

$$co\varphi(a) - a^{\frac{m-1}{m}} = p^{e-1} - p^{\frac{em-e}{m}}$$

$e - 1 - \frac{em-e}{m} = \frac{e-m}{m} \geq 0$ により, 上式は非負.
等号成立は $a = p^m$ のとき.

2. $r \geq 2$.
$P, R, \overline{P}$ を次式で定義する.
$P = \prod_{j=1}^{r} p_j, R = \prod_{j=1}^{r} p_j^{e_j - 1}, \overline{P} = \prod_{j=1}^{r} \overline{p_j},$ を以下で用いる.
$a = PR, \varphi(a) = \overline{P}R$ が成り立つ. それゆえ

$$\begin{aligned} co\varphi(a) - a^{\frac{m-1}{m}} &= co\varphi(a) - \frac{a}{a^{\frac{1}{m}}} \\ &= PR - \overline{P}R - \frac{PR}{a^{\frac{1}{m}}} \end{aligned}$$

この式を R で割ると

$$(co\varphi(a) - a^{\frac{m-1}{m}})/R = P - \overline{P} - \frac{P}{a^{\frac{1}{m}}}.$$

$j > 1$ について $p_1 < p_j()$ なので $p_1^{\frac{e_j}{m}} < p_j^{\frac{e_j}{m}}$.
j について 1 から r について上の式を掛けると

$$p_1^{\frac{\varepsilon(a)}{m}} \leq \prod p_j^{\frac{e_j}{m}} = a^{\frac{1}{m}}.$$

ゆえに $r > 1$ のとき $\varepsilon(a) \geq m$ により

$$a^{\frac{1}{m}} \geq p_1^{\frac{\varepsilon(a)}{m}} \geq p_1.$$

$$P-\overline{P}-\frac{P}{a^{\frac{1}{m}}}\geq P-\overline{P}-\frac{P}{p_1}.$$

$P_0=\prod_{j=2}^{r}p_j$ とおくとき $P=p_1P_0$. また $p_1=\overline{p_1}+1$ により $\overline{P_0}=\prod_{j=2}^{r}\overline{p_j}$ とおくと

$$\begin{aligned}P-\overline{P}-\frac{P}{p_1}&=(\overline{p_1}+1)P_0-\overline{P}-P_0\\&=\overline{p_1}P_0-\overline{p_1}\overline{P_0}\\&=\overline{p_1}(P_0-\overline{P_0})>0.\end{aligned}$$

ゆえに

$$\begin{aligned}(co\varphi(a)-a^{\frac{m-1}{m}})/R=P-\overline{P}-\frac{P}{a^{\frac{1}{m}}}\\\geq\overline{p_1}(P_0-\overline{P_0})>0.\end{aligned}$$

0.4　60 進法

0.4.1　(Wikipedia)

60 進法にもとづいた位取り記数法を作りあげ、バビロニア数学の発展のもとになった。紀元前 3000 年頃のシュメール時代の記数法には系統的な 60 進法はなかった

紀元前 2000 年頃に「1」と「10」を表す記号によって 60 進記数法が用いられるようになった。

分数の簡潔な表現も可能とし、小数の概念も存在した。

基数が 60 で位取り方式があったため計算が容易になり、特に分数計算が簡便となった。計算を簡潔にするために、逆数、平方、立法、乗法などを数表にした。乗算表には、2 から 20、そして 30、40、50 の掛け算が載っていた。

逆数表には、81 までの整数では 2、3、5 の倍数のみ掲載することが多く、60 の因数ではない素数（7、11 等）の逆数は除外された。

0.4.2　(室井和男)

古代バビロニア時代の標準的な逆数表は, 分母が, 2,3,5 で構成されたものに限っているがシュメール由来の逆数表では 42 の逆数は求まらない, と書かれている.

1/42,1/7 の 60 進展開は次のとおり.

```
1 ?-  j(1/42,60).
0.   1   25   42   51   25   42   51   25   42   51
2 ?- j(1/7,60).
0.   8   34   17   8   34   17   8   34   17   8   34   17

3 ?- j(1/12,60).
0.   5
```

シュメール人は 7 の逆数がはじめて循環小数になることに気づいた. 7 は神聖なもので人間の力では計り知れない何らかの性質を持つと考えた. そして 7 を神秘な数と認識した.

室井和男著　『シュメール人の数学』 共立出版, 2017

シュメール人は今から 4000 年以上昔の時代分数の 60 進展開を行いまた逆数の計算を行い逆数の数表を作った.

小手調べに次の 分数の 60 進展開を行う.

```
15 ?- lj(1/7,60,A,B).
A = [8, 34, 17],
B = [4, 2, 1].
```

1/7 を 60 進展開する計算を行うと, 8, 34, 17,8, 34, 17,8, 34, 17,$\cdots$ が無限に続くことにシュメール人は今から 4000 年以上昔に気づきそれを楔形文字で粘土板に焼き付けた.

粘土板は歳月を重ねてより強固になり,20 世紀に発見されその解読が行われた.

A $=$ [8, 34, 17] は長さが 3 の循環節である.

私は最初のうち, 1/7 を 60 進法で計算することがなかなかできなかった.
循環節 [8, 34, 17] は 3 個の数からなる
3 は素数だから, 半分に分けて足すなどはできない.
そこでこれらを足してみた
8+ 34+ 17=59
59 になった.$59-1=60$ という関係がある.

```
6 ?- lj(1/1198151,60,A,B).
A = [0, 0, 0, 10, 49],
B = [60, 3600, 216000, 978490, 1].

5 ?- lj(100/1198151,60,A,B).
A = [0, 0, 18, 1, 40],
B = [6000, 360000, 33282, 798769, 100].

6 ?- lj(1/1198151,60,A,B).
A = [0, 0, 0, 10, 49],
B = [60, 3600, 216000, 978490, 1].

7 ?- lj(1000/1198151,60,A,B).
A = [0, 3, 0, 16, 40],
B = [60000, 5547, 332820, 798784, 1000].

8 ?- lj(100000/1198151,60,A,B).
A = [5, 0, 27, 46, 40],
B = [9245, 554700, 931923, 800434, 100000].
```

少し一般にして, 60 を一般の $g>1$ にして 既約分数 $\frac{a}{b}, a<b$ を g 進展開する.
長さが 3 の循環節とすると, 計算は 次の通り

- $ga=q_1b+r_1$, ; 分子 a を g 倍して, 分子 b で割って商を q_1, 余りを r_1 とする.
- $gr_1=q_2b+r_2$, ; r_1 を g 倍して, 分子 b で割って商を q_2, 余りを r_2 とする.
- $gr_2=q_3b+r_3$,; r_2 を g 倍して, 分子 b で割って商を q_3, 余りを r_3 とする.

$r_3=r_0(r_0=a)$ となりこれが長さが 3 の循環節の意味である.
$R=r_0+r_1+r_2, Q=q_1+q_2+q_3$ とおき上の 3 式を加える.
$gR=Qb+R$ になり, $(g-1)R=Qb$.
素数 b は $g-1$ または R を割る.
$g-1=sb$ なら $g\equiv 1 \mod b$. 長さが 1 になり矛盾.
$R=sb$ となる. $r_j<b$ なので $sb=R<3b-1$. により $s=1,2$.

ここで, $a = 1$ と仮定すると, $R = 1 + r_1 + r_2 < 1 + b + b - 1 = 2b$ なので $R = b$. ゆえに, $g - 1 = Q$. すなわち商をみな足すと, $g - 1$ になる.

$a > 1$ なら $s = 2$ は起きてそのとき, $2(g - 1) = Q$.

$< q_1, q_2, q_3 > /g = q_1 g^2 + q_2 g + q_3$ とおく.

- $g^3 a = g^2 q_1 b + g^2 r_1$,
- $g^2 r_1 = g q_2 b + g r_2$,
- $g r_2 = q_3 b + r_3$,;

すなわち上の段では g^2, 中の段では g を掛け, 下の段はそのままにして足すと見事に打ち消しあって,

$\widetilde{Q} =< q_1, q_2, q_3 > /g = q_1 g^2 + q_2 g + q_3$ とおくと

$g^3 a = b\widetilde{Q} + a$, $(a = r_3)$ を得る.

$(g^3 - 1)a = b\widetilde{Q}$ であり, 素数 b は $(g - 1)a$ を割ることはないので $g^2 + g + 1 = tb$ となり,

$(g - 1)at = \widetilde{Q}$.

$a = 1$ すなわち真分数なら, $(g - 1)t = \widetilde{Q}$. $\widetilde{Q}$ も $g - 1$ の倍数である.

```
16 ?- lj(1/11,60,A,B).
A = [5, 27, 16, 21, 49],
B = [5, 3, 4, 9, 1].


3 ?- lj(1/11,60,A,B).
A = [5, 27, 16, 21, 49],

B = [5, 3, 4, 9, 1].
```

循環節 [5, 27, 16, 21, 49] は 5 個の数からなる
5 は素数だから, 半分に分けて足すなどはできない.
そこでこれらを足してみた

0.5　10 進展開

分数とくに単位分数を 10 進展開することは計算練習になり、脳の活性化に大きく寄与する.

100 マス計算のごとくひたすら耐えて計算することと異なりこれらの分数の計算で循環節を求めることは実に面白い.

循環節が偶数の長さなら, 循環節を半分に割って足す.

```
1 ?-  lj(1/7,10,A,B).
A = [1, 4, 2, 8, 5, 7], (循環節)
B = [3, 2, 6, 4, 5, 1]. (余りの節)

2 ?- lj(1/13,10,A,B).
A = [0, 7, 6, 9, 2, 3],
B = [10, 9, 12, 3, 4, 1].
```

(循環節) [1, 4, 2, 8, 5, 7] や (余りの節) の数の個数が偶数なら半分に分けて
できた [1, 4, 2],[8, 5, 7] を足してみよう.

(余りの節)[3, 2, 6, 4, 5, 1] の個数が偶数なら半分に分けて
できた [3, 2, 6] と [4, 5, 1]　を足してみよう.

同様に数の個数が 3 の倍数なら 3 で割って足す.

```
13 ?- lj(1/19,10,A,B).
A = [0, 5, 2, 6, 3, 1, 5, 7, 8, 9, 4, 7, 3, 6, 8, 4, 2, 1],
B = [10, 5, 12, 6, 3, 11, 15, 17, 18, 9, 14, 7, 13, 16, 8, 4, 2, 1].

7 ?- lj(1/37,10,A,B).
A = [0, 2, 7],
B = [10, 26, 1].
```

1/37 の場合は例外的に簡単になる.

0.6　5 進展開

5 進展開での計算はなれないとなかなかできない.

```
4 ?- lj(1/7,5,A,B).
A = [0, 3, 2, 4, 1, 2],
B = [5, 4, 6, 2, 3, 1].

5 ?- lj(1/11,5,A,B).
A = [0, 2, 1, 1, 4],
B = [5, 3, 4, 9, 1].

14 ?- lj(1/19,5,A,B).
A = [0, 1, 1, 2, 4, 2, 1, 4, 1],
B = [5, 6, 11, 17, 9, 7, 16, 4, 1].
```

循環節が偶数の長さなら, 循環節を半分に割って足す.