書泉グランデでの講義
高校生も十分わかる新しい数論研究 New Series, 第 1 期
資料 0
2015 年 10 月 23 日

飯高 茂

平成 27 年 10 月 17 日

第1章　準備編

10・9 では配布資料 1 で説明する予定でしたが、オイラー関数について詳しく解説する必要があると思い循環小数の話題から解説しました。そのとき配布資料が間に合いませんでした。ここに、資料 0 としてお届けします.

1.1　循環小数から

swi-prolog での結果を最初に展示します.

```
?-  1/7 = 0.
142857142857142857142857142857142857142857142857142857
```

```
 25 ?- 1/17=
0.
058823529411764705882352941176470588235294117647058823529411764705882352941176470588235294117647
```

循環節の長さは興味がある対象でここにオイラー関数が出てきます.
$1/7, 1/17, 1/13$ を 10 進で展開したときの, 商の列 X とあまりの列 Y を表示しました.

```
19 ?- lj(1/7,10,X,Y),write(X),nl,write(Y),nl.
[1,4,2,8,5,7]
[3,2,6,4,5,1]
X = [1, 4, 2, 8, 5, 7],
Y = [3, 2, 6, 4, 5, 1].
```

```
18 ?- lj(1/17,10,X,Y),write(X),nl,write(Y),nl.
[0,5,8,8,2,3,5,2,9,4,1,1,7,6,4,7]
[10,15,14,4,6,9,5,16,7,2,3,13,11,8,12,1]
X = [0, 5, 8, 8, 2, 3, 5, 2, 9|...],
Y = [10, 15, 14, 4, 6, 9, 5, 16, 7|...].
```

```
20 ?-   lj(1/13,10,X,Y),write(X),nl,write(Y),nl.
```

```
[0,7,6,9,2,3]
[10,9,12,3,4,1]
X = [0, 7, 6, 9, 2, 3],
Y = [10, 9, 12, 3, 4, 1].
```

10 進展開なら分母が 2,5 で割れない素数 p なら循環節の長さは $p-1$ の約数

一般に G 進展開なら分母が G と互いに素で 分数が真の既約分数 $\frac{a}{b}$ ならその小数展開は最初から循環し (純循環) 循環節の長さはオイラー関数 $\varphi(b)$ の約数

$\frac{a}{b} = \frac{1}{50}$ の 11 進展開,3 進展開,7 進展開 を行っています.

$\varphi(50) = \varphi(2)\varphi(25) = 20$ 20 の 約数は 5,4,2,1.25

$\frac{a}{b} = \frac{1}{100}$ の 7 進展開,3 進展開,11 進展開 を行っています.

```
16 ?- lj0(1/50,11,J).
[0,2,4,6,9]
J = [0, 2, 4, 6, 9].

17 ?- lj0(1/50,3,J).
[0,0,0,1,1,2,1,2,0,1,2,2,2,1,1,0,1,0,2,1]
J = [0, 0, 0, 1, 1, 2, 1, 2, 0|...].

18 ?- lj0(1/50,7,J).
[0,0,6,6]
J = [0, 0, 6, 6].

19 ?- lj0(1/100,7,J).
[0,0,3,3]
J = [0, 0, 3, 3].

20 ?- lj0(1/100,3,J).
[0,0,0,0,2,1,0,2,1,2,1,1,1,0,2,0,0,1,2,2]
J = [0, 0, 0, 0, 2, 1, 0, 2, 1|...].

21 ?- lj0(1/100,11,J).
[0,1,2,3,4,5,6,7,8,10]
J = [0, 1, 2, 3, 4, 5, 6, 7, 8|...].
```

1.2　オイラー関数

n を法とするとき乗法群 ${\mathbb{Z}_n}^*$ の元の個数をオイラー関数と言う

分数の概念だけでもオイラー関数が定義できる.

自然数を分母, 分子に持つ分数を考える. 分母が n の真分数は $\frac{a}{n}; (1 \leq a \leq n)$ なので合計 n 個ある.

例えば $n = 6$ なら

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6} \tag{1.1}$$

$\frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{6}{6}$ らは可約分数. $\frac{1}{6}, \frac{5}{6}$ は既約分数

$\frac{a}{n}$ のうち既約分数になるものの個数を $\varphi(n)$ で表し**オイラー関数**という.

たとえば $n = 12$ なら $\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}$ のみが既約分数だから $\varphi(12) = 4$.

a, b が互いに素なら $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これを オイラー関数の乗法性という.

a が素数べき p^e のとき $\varphi(a) = \varphi(p^e) = \frac{a(p-1)}{p}$ と書けるから $p\varphi(a) = (p-1)a$ を満たす. $p = 2$ なら $2\varphi(a) = a$ となって,$\sigma(a) = 2a - 1$ と見かけが似ている.

1.2.1 オイラー関数数表

表 1.1:

a	素因数分解	$s(a)$	$\varphi(a)$	a	素因数分解	$s(a)$	$\varphi(a)$
2	$[2]$	1	1	27	$[3^3]$	1	18
3	$[3]$	1	2	28	$[2^2, 7]$	2	12
4	$[2^2]$	1	2	29	$[29]$	1	28
5	$[5]$	1	4	30	$[2, 3, 5]$	3	8
6	$[2, 3]$	2	2	31	$[31]$	1	30
7	$[7]$	1	6	32	$[2^5]$	1	16
8	$[2^3]$	1	4	33	$[3, 11]$	2	20
9	$[3^2]$	1	6	34	$[2, 17]$	2	16
10	$[2, 5]$	2	4	35	$[5, 7]$	2	24
11	$[11]$	1	10	36	$[2^2, 3^2]$	2	12
12	$[2^2, 3]$	2	4	37	$[37]$	1	36
13	$[13]$	1	12	38	$[2, 19]$	2	18
14	$[2, 7]$	2	6	39	$[3, 13]$	2	24
15	$[3, 5]$	2	8	40	$[2^3, 5]$	2	16
16	$[2^4]$	1	8	41	$[41]$	1	40
17	$[17]$	1	16	42	$[2, 3, 7]$	3	12
18	$[2, 3^2]$	2	6	43	$[43]$	1	42
19	$[19]$	1	18	44	$[2^2, 11]$	2	20
20	$[2^2, 5]$	2	8	45	$[3^2, 5]$	2	24
21	$[3, 7]$	2	12	46	$[2, 23]$	2	22
22	$[2, 11]$	2	10	47	$[47]$	1	46
23	$[23]$	1	22	48	$[2^4, 3]$	2	16
24	$[2^3, 3]$	2	8	49	$[7^2]$	1	42
25	$[5^2]$	1	20	50	$[2, 5^2]$	2	20
26	$[2, 13]$	2	12	51	$[3, 17]$	2	32

表 1.2:

a	素因数分解	$s(a)$	$\varphi(a)$	a	素因数分解	$s(a)$	$\varphi(a)$
2	$[2]$	1	1	32	$[2^5]$	1	16
3	$[3]$	1	2	34	$[2, 17]$	2	16
4	$[2^2]$	1	2	40	$[2^3, 5]$	2	16
6	$[2, 3]$	2	2	48	$[2^4, 3]$	2	16
5	$[5]$	1	4	60	$[2^2, 3, 5]$	3	16
8	$[2^3]$	1	4	19	$[19]$	1	18
10	$[2, 5]$	2	4	27	$[3^3]$	1	18
12	$[2^2, 3]$	2	4	38	$[2, 19]$	2	18
7	$[7]$	1	6	54	$[2, 3^3]$	2	18
9	$[3^2]$	1	6	25	$[5^2]$	1	20
14	$[2, 7]$	2	6	33	$[3, 11]$	2	20
18	$[2, 3^2]$	2	6	44	$[2^2, 11]$	2	20
15	$[3, 5]$	2	8	50	$[2, 5^2]$	2	20
16	$[2^4]$	1	8	66	$[2, 3, 11]$	3	20
20	$[2^2, 5]$	2	8	23	$[23]$	1	22
24	$[2^3, 3]$	2	8	46	$[2, 23]$	2	22
30	$[2, 3, 5]$	3	8	35	$[5, 7]$	2	24
11	$[11]$	1	10	39	$[3, 13]$	2	24
22	$[2, 11]$	2	10	45	$[3^2, 5]$	2	24
13	$[13]$	1	12	52	$[2^2, 13]$	2	24
21	$[3, 7]$	2	12	56	$[2^3, 7]$	2	24
26	$[2, 13]$	2	12	70	$[2, 5, 7]$	3	24
28	$[2^2, 7]$	2	12	72	$[2^3, 3^2]$	2	24
36	$[2^2, 3^2]$	2	12	78	$[2, 3, 13]$	3	24
42	$[2, 3, 7]$	3	12	84	$[2^2, 3, 7]$	3	24
17	$[17]$	1	16	90	$[2, 3^2, 5]$	3	24

1.3　オイラー関数の基本性質

ただし $\varphi(1)=1$ とする. オイラー関数 $\varphi(a)$ の性質 ($a>1$) を列挙しよう.

1. $a-1 \geq \varphi(a)$,
2. a が素数なら $\varphi(a)=a-1$. さらに $\varphi(a)=a-1$ なら a は素数 ,
3. a が素数でないなら $a \geq \varphi(a)+\sqrt{a}$,
4. a,b が互いに素なら $\varphi(ab)=\varphi(a)\varphi(b)$ (乗法性).

1.3.1　オイラーの公式

オイラー関数に関した次の公式は定義からすぐ導かれる.

$$a=\sum_{a'|a}\varphi(a') \tag{1.2}$$

ここに $a'|a$ は a' が a の約数を意味する. これを**オイラーの公式**という.

たとえば $a=12$ とおくと,$a'=12,6,4,3,2,1$ であり ,

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

これらを加えると $4+2+2+2+1+1=12$ となって分母 12 が出て来る.

この公式を使うと, オイラー関数 $\varphi(a)$ の値が機械的に計算できる.

a が素数の平方 p^2 なら約数は $p^2,p,1$ なので $p^2=\varphi(p^2)+\varphi(p)+1=\varphi(p^2)+(p-1)+1$ により $\varphi(p^2)=p^2-p=p(p-1)$.

同様にして $\varphi(p^e)=p^e-p^{e-1}=p^{e-1}(p-1)$ が示される.

p,q を相異なる素数とすると pq の約数は $pq,q,p,1$ なので $pq=\varphi(pq)+\varphi(q)+\varphi(p)+1=\varphi(pq)+(q-1)+(p-1)+1$ により $\varphi(pq)=pq-p-q+1=(p-1)(q-1)$.

1.3.2　乗法性

a, b を互いに素な自然数とするとき, $\varphi(ab) = \varphi(a)\varphi(b)$ が成り立つ. これがオイラー関数の乗法性である. ここでは高校の数学 I にある集合の数え方を用いた簡単な証明方法を述べよう.

1.3.3　乗法性の証明

$a > 1$ に対して a 以下の自然数の集合を $S(a)$ と書く. a の素因子 p について, $S(a)$ 内の p の倍数全体は $pS(a/p)$ と書くことができる. ここで自然数の集合 T についてその元の p 倍数全体を pT で示した. たとえば $2\{1,2,3\} = \{2,4,6\}$.

a の相異なるすべての素因子を $p_1, \cdots, p_s$ とする. $A_j = p_j S(a/p_j)$ とおくとき和集合 $A_1 \cup \cdots \cup A_s$ に属さない $S(a)$ の元 b は a 未満で a と互いに素な自然数である. したがって $A_1 \cup \cdots \cup A_s$ の $S(a)$ についての補集合の元の個数が オイラー関数の値 $\varphi(a)$ である.

有限集合 T の元の個数を絶対値記号を流用して $|T|$ で示すとき $\varphi(a) = a - |A_1 \cup \cdots \cup A_s|$ と書ける.

$p = p_j$ とおくとき $|A_j| = \frac{a}{p}$ になる.

簡単のため, $s = 2, p = p_1, q = p_2$ とすると $A_1 \cap A_2 = pqS(a/pq)$ によって $|A_1 \cap A_2| = \frac{a}{pq}$.

ゆえに

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

を用いると

$$\begin{aligned}\varphi(a) = a - |A_1 \cup A_2| &= a - |A_1| - |A_2| + |A_1 \cap A_2| \\ &= a - \frac{a}{p} - \frac{a}{q} + \frac{a}{pq} \\ &= a(1 - \frac{1}{p})(1 - \frac{1}{q})\end{aligned}$$

書き直すと

$$\varphi(a) = a(1 - \frac{1}{p})(1 - \frac{1}{q})$$

$a = p^e q^f$ と書くとき

$$\varphi(a) = a(1 - \frac{1}{p})(1 - \frac{1}{q}) = p^e(1 - \frac{1}{p})q^f(1 - \frac{1}{q}) = p^{e-1}\overline{p}q^{f-1}\overline{q}$$

となる. ここで $\overline{p} = p - 1, \overline{q} = q - 1$.

一般には 素因数分解して $a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ のように相異なる素数 $p_1, p_2, \cdots, p_s$ のべきの積で書くと次のようになる:

$$\varphi(a) = p_1^{e_1-1}\overline{p_1}p_1^{e_2-1}\overline{p_2}\cdots p_s^{e_s-1}\overline{p_s}.$$

これからオイラー関数の乗法性は直ちに導かれる.

1.4　オイラー関数について 3 点セット

オイラー関数について 3 点セットを考える.

1. $2\varphi(a)-a=0$ を満たす自然数 a は何か.
2. $2\varphi(a)-a=1$ を満たす自然数 a は何か.
3. $2\varphi(a)-a=-1$ を満たす自然数 a は何か.

1 番目の a は 2^e になることが示される.
実際, $2\varphi(a)=a$ とすると a は偶数なので $a=2^eL(L$:奇数$)$ と書ける.

$$\varphi(a)=\varphi(2^e)\varphi(L)=2^{e-1}\varphi(L)$$

なので, $2\varphi(a)=2^e\varphi(L)$. 条件式 $2\varphi(a)=a=2^eL$ によれば

$$2^e\varphi(L)=2^eL$$

$\varphi(L)=L$ になり, $L=1$. すなわち $a=2^e$.

1.5　フェルマー数

$m=2^e$ について $f=2^m$ を f_e とし さらに $F_e=f_e+1$ と書いてこれをフェルマー数という.
$F_0=3,F_1=5,F_2=17,F_3=257,F_4=65537$ はみな素数でこれらをフェルマー素数という.
これら 5 つの素数をまとめてフェルマー素数 5 兄弟, と呼ぼう.
$j\leq 4$ に関して $a_j=F_0F_1\cdots F_j$ とおくとき

$$\varphi(a_j)=f_0f_1\cdots f_j=2^{1+2+\cdots 2^j}=2^{2^{j+1}-1}$$

$$2\varphi(a_j)=f_{j+1}.$$

一方, $(f_j)^2=f_{j+1}$ により

$$(f_j)^2-1=f_{j+1}-1, f_{j+1}-1=(f_j)^2-1=(f_j-1)F_j$$

これより $f_{j+1}-1=F_0F_1\cdots F_j=a_j$. ゆえに $2\varphi(a_j)=f_{j+1}=a_j+1$. すなわち $2\varphi(a_j)-a_j=1$ を満たす. $2\varphi(a)-a=1$ を満たす自然数 a としてはこれらの $a_0,a_1,\cdots,a_4$ だけが知られている.
手計算で確認しよう.

1. $a_0=3,\varphi(3)=2$. このとき $2\varphi(3)-3=1$.
2. $a_1=3*5=15,\varphi(15)=8$. このとき $2\varphi(15)-15=1$.
3. $a_2=3*5*17=255,\varphi(255)=128$. このとき $2\varphi(255)-255=1$.

表 1.3: $a - 2\varphi(a) = -1$ の表

a	$\varphi(a)$	素因数分解
3	2	[3]
15	8	[3, 5]
255	128	[3, 5, 17]
65535	32768	[3, 5, 17, 257]
4294967295	7304603328	[3, 5, 17, 257, 65537]

$a - 2\varphi(a) = -1$ の解にフェルマー素数の 5 兄弟が順に出てくる．これはきわめて美しい結果といわざるを得ない．

問題にすべきことはこの逆である. すなわち, $2\varphi(a)-a=1$ を満たす a はこれらの 5 個の数しかないか?.

これを示すため最初に $2\varphi(a)-a=1$ を満たす a に平方因子がないことを示す.

実際, $a=p^eb$,$e>1$, b は p で割れないとする. $\varphi(a)-a$ は p^{e-1} を因子としてもつが, 右辺は 1 なので矛盾.

$a=p_1p_2\cdots p_s$ とおくとき $\overline{p_1}=p_1-1$ を使うと

$\varphi(a)=\overline{p_1p_2}\cdots\overline{p_s}$ により

$$2\overline{p_1p_2}\cdots\overline{p_s}-p_1p_2\cdots p_s=1$$

を解けばよい.

n を自然数とするとき,n を法とした整数の剰余環の乗法群 $\mathbb{Z}_n{}^*$ の元の数が $\varphi(n)$ になっている.

例えば,$\varphi(4)=2,\varphi(6)=2,\varphi(29)=28$ など.

p が素数なら $\varphi(p)=p-1$. これは p が 素数になる必要十分条件である.

1.5.1 オイラー関数の等式

$\mathrm{GCD}(n,a)=d$ のとき $n=n'd, a=a'd$ と書くと, $\dfrac{a}{n}=\dfrac{a'}{n'}$.

すなわち, n' は n の約数である. このようにして，可約分数 $\dfrac{a}{n}$ は n の約数 n' を分母にもつ既約分数 $\dfrac{a'}{n'}$ になるので, これらは $\varphi(n')$ 個ある. n' が約数のとき $d=n/n'$ も約数なので, 最初の既約分数の個数も合わせて足せばもとの分数の総数 n が得られる.n' をあらためて d と書き換えると次の公式をえる.

$$\sum_{d|n}\varphi(d)=n \tag{1.3}$$

記号 $d|n$ は d が n の**約数であること**を意味する [1] .

$n=6$ の場合その約数は 1,2,3,6 であり

$$\varphi(1)=1,\varphi(2)=1,\varphi(3)=2,\varphi(6)=2.$$

このとき 1+1+2+2=6.

オイラー関数の等式を使うと, オイラー関数の値が求められる.

p を素数として $n=p^2$ とおく. その約数は $1,p,p^2$ なので

$$\varphi(1)+\varphi(p)+\varphi(p^2)=p^2.$$

$\varphi(1)=1,\varphi(p)=p-1$ なので $r>1$ のとき $\varphi(p^r)=p^r-p^{r-1}=p^{r-1}(p-1)$.

q を p と異なる素数とし $n=pq$ とおく. その約数は $1,p,q,pq$. オイラー関数の等式によれば

$$\varphi(1)+\varphi(p)+\varphi(q)+\varphi(pq)=pq.$$

これより

$$\varphi(pq)=pq-(p-1+q-1+1)=(p-1)(q-1).$$

これを使えば,

$$\varphi(21)=12,\varphi(5\cdot 29)=4\cdot 28=112.$$

などがわかる.

[1] 英語では d divides n, という. 日本語でも d 割る n と読むことがある.

10 進展開分母の素因数分解と周期 (循環節の長さ)
分母が素数 p なら 周期は $p-1$ の約数
分母が数 m なら 周期は $\varphi(m)$ の約数
周期を簡単に知る方法はない.
$1/m$ の 10 進展開での循環節の長さ (period): m の素因数分解との関連

```
3=[3]      period=1       euler=2
7=[7]      period=6       euler=6
9=[3^2]      period=1     euler=6
11=[11]      period=2     euler=10
13=[13]      period=6     euler=12
17=[17]      period=16    euler=16
19=[19]      period=18    euler=18
21=[3,7]      period=6    euler=12
23=[23]      period=22    euler=22
27=[3^3]      period=3    euler=18
29=[29]      period=28    euler=28
31=[31]      period=15    euler=30
33=[3,11]      period=2   euler=20
37=[37]      period=3     euler=36

39=[3,13]      period=6   euler=24
41=[41]      period=5     euler=40
43=[43]      period=21    euler=42
47=[47]      period=46    euler=46
49=[7^2]      period=42   euler=42

51=[3,17]      period=16  euler=32
53=[53]      period=13    euler=52
57=[3,19]      period=18  euler=36
59=[59]      period=58    euler=58
61=[61]      period=60    euler=60
63=[3^2,7]      period=6  euler=36
67=[67]      period=33    euler=66
69=[3,23]      period=22  euler=44
71=[71]      period=35    euler=70
73=[73]      period=8     euler=72
77=[7,11]      period=6   euler=60
79=[79]      period=13    euler=78
```

5 進展開分母の素因数分解と周期 (循環節の長さ)

```
2=[2]     period=1      euler=1
3=[3]     period=2      euler=2
4=[2^2]     period=1    euler=2
6=[2,3]     period=2    euler=2
7=[7]     period=6      euler=6
8=[2^3]     period=2    euler=4
9=[3^2]     period=6    euler=6
11=[11]     period=5    euler=10
12=[2^2,3]     period=2 euler=4
13=[13]     period=4    euler=12
14=[2,7]     period=6   euler=6
16=[2^4]     period=4   euler=8
17=[17]     period=16   euler=16
18=[2,3^2]     period=6 euler=6
19=[19]     period=9    euler=18
21=[3,7]     period=6   euler=12
22=[2,11]     period=5  euler=10
23=[23]     period=22   euler=22
24=[2^3,3]     period=2 euler=8
26=[2,13]     period=4  euler=12
27=[3^3]     period=18  euler=18
29=[29]     period=14   euler=28
31=[31]     period=3    euler=30
32=[2^5]     period=8   euler=16
33=[3,11]     period=10 euler=20
34=[2,17]     period=16 euler=16
36=[2^2,3^2]     period=6       euler=12
37=[37]     period=36   euler=36
38=[2,19]     period=9  euler=18
39=[3,13]     period=4  euler=24
41=[41]     period=20   euler=40
42=[2,3,7]     period=6 euler=12
43=[43]     period=42   euler=42
44=[2^2,11]     period=5        euler=20
46=[2,23]     period=22 euler=22
47=[47]     period=46   euler=46
48=[2^4,3]     period=4 euler=16
49=[7^2]     period=42  euler=42
```

2 進展開分母の素因数分解と周期 (循環節の長さ)

```
3=[3]     period=2      euler=2
5=[5]     period=4      euler=4
7=[7]     period=3      euler=6
9=[3^2]     period=6    euler=6
11=[11]     period=10   euler=10
13=[13]     period=12   euler=12
15=[3,5]     period=4   euler=8
17=[17]     period=8    euler=16
19=[19]     period=18   euler=18
21=[3,7]     period=6   euler=12
23=[23]     period=11   euler=22
25=[5^2]     period=20  euler=20
27=[3^3]     period=18  euler=18
29=[29]     period=28   euler=28

31=[31]     period=5    euler=30
33=[3,11]     period=10 euler=20
35=[5,7]     period=12  euler=24
37=[37]     period=36   euler=36
39=[3,13]     period=12 euler=24
41=[41]     period=20   euler=40
43=[43]     period=14   euler=42
45=[3^2,5]     period=12        euler=24
47=[47]     period=23   euler=46
49=[7^2]     period=21  euler=42
```

1.6　オイラー関数

互いに素な自然数 n, m に対して

$$\varphi(nm) = \varphi(n)\varphi(m). \tag{1.4}$$

この性質を**オイラー関数の乗法性**という.

一般に自然数 n の相異なる素因数を $p_1, p_2, \cdots, p_s$ とおくと指数 $e_1, e_2, \cdots, e_s$ により素因数分解

$$n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$$

できる. これより

$$\varphi(n) = \varphi({p_1}^{e_1})\varphi({p_2}^{e_2})\cdots\varphi({p_s}^{e_s}).$$

$\varphi({p_1}^{e_1}) = {p_1}^{e_1} - {p_1}^{e_1-1}, \cdots$ に注意すると

$$\varphi(n) = n(1 - {p_1}^{-1})(1 - {p_2}^{-1})\cdots(1 - {p_s}^{-1}).$$

をえる. これを**オイラーの公式**という.

例

1. $\varphi(10) = \varphi(2)\varphi(5) = 4,$
2. $\varphi(100) = \varphi(2^2)\varphi(5^2) = 40,$
3. $\varphi(1000) = \varphi(2^3)\varphi(5^3) = 400.$

このように自然数 n の素因数分解が出来れば $\varphi(n)$ の計算は簡単にできるが $\varphi(n)$ の逆を求めること, すなわち, 与えられた m に対して $\varphi(n) = m$ を満たす n を求めることは簡単でない.