オイラー 関数と オイラー 完全数

飯高 茂

平成 28 年 10 月 9 日

1　素因数分解の定理

自然数の世界で素因数分解の一意性定理が成り立つことはユークリッドらのすでに知ることであるが１８世紀の終わりごろガウスがこの定理の証明が不完全であることを嘆いて次の結果を D.A. で証明している.

補題
p が素数で a, b 自然数のとき $ab \equiv 0 \mod p$ なら $a \equiv 0$ または $b \equiv 0 \mod p$ となる.

背理法で示すため $ab \equiv 0 \mod p$ のとき $a \not\equiv 0$ かつ $b \not\equiv 0 \mod p$ を仮定する.
ここで, a, p を固定して考える. 上記を満たす b の中で最小に選ぶ. p を b で割るときその商とあまりを 自然数 Q と r で示すと $p = bQ + r, r < b$.
$ab = pm$ と書いてから $p = bQ + r$ を a 倍すると
$ap = abQ + ar = pmQ + ar$.
$p(a - mQ) = ar$ なので $m' = a - mQ$ とおくとき $ar = pm', 0 \leq r < b$.
b は最小値なので $r = 0$.
ゆえに $p = bQ$. p は素数なので $Q = 1; p = b$. 仮定:$b \not\equiv 0 \mod p$ に反する.

$R = Z$ を整数環とする. 環論のことばを使うと $J = pR$ を p の倍数イデアルとすると, J は極大イデアル. したがって J も素イデアルになる.
これがガウスの補題の意味である.

伝統的な証明法は素数 p に対し、イデアル $J = pZ$ が極大イデアルになることを示す.
a が $J = pZ$ に属さないとき p で割れない. a と p の最大公約数は 1 なので $1 = am + pn$ を満たす整数 n, m がある.
これは a と J の生成するイデアルが全体になることを意味する. したがって, J は素イデアル.

2　究極の完全数とその平行移動

オイラー 完全数を導入する前に究極の完全数の定義を復習する.

$\sigma(a)$ を自然数 a の約数の和として, $\sigma(a)$ を関数と見て ユークリッド関数という.

P を素数とし, 整数 m に関して $\sigma(P^e)+m$ が素数 q のとき $a=P^eq$ を m だけ平行移動した底が P の狭義の究極の完全数と呼ぶ.

これは次式を満たす.

$$\overline{P}\sigma(a)-Pa=(P-2)\mathrm{Maxp}(a)-m(P-1). \tag{1}$$

$\mathrm{Maxp}(a)$ は a の最大素因子を指している.

この式を満たす a を m だけ平行移動した底が P の広義の究極の完全数と呼ぶ.

3 φ 完全数

究極の完全数の定義を参考にユークリッド関数の代わりに自然数 a と互いに素で a 未満の自然数の個数を示すオイラー関数 $\varphi(a)$ を使って完全数と類似した概念を定義しよう.

しかしながら $\varphi(P^e),(e>1)$ は合成数なので完全数の定義をそのままは使えない. そこで, 1 を加えて $\varphi(P^e)+1$ が素数 q になるとき $a=P^eq$ をもって P を底とする狭義のオイラー φ 完全数と定義する.

さて最も簡単な　$P=2$ の場合を定義に沿ってパソコンで計算してみる.

表 1: $P=2$ を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	2^2*3	4
3	40	2^3*5	16
5	544	2^5*17	256
9	131584	2^9*257	65536
17	8590065664	$2^{17}*65537$	4294967296

計算の結果,a の素数部分には 3,5,17,257,65537 のようにフェルマ素数が並んでいるではないか.

しかし, 定義に戻ると, $q=\varphi(P^e)+1=2^{e-1}+1$ が素数という条件になるので $e-1=2^m$ と書けて q がフェルマ素数になるのは当然である.

4　オイラー φ 完全数の平行移動

m だけ平行移動した オイラー φ 完全数の定義は次の通り.

$\varphi(P^e)+1+m, e>1$ が素数 q になるとき $a=P^eq, e\geq 2$ を (P を底とする) m だけ平行移動した (狭義の) オイラー φ 完全数の定義とする.

特にこれを満たす a を (φ, m) 完全数とも言う.

5　オイラーの φ 完全数の方程式

つぎにオイラーの φ 完全数の方程式を導入する.

$q=\varphi(P^e)+1+m$ を素数とし $a=P^eq$ をオイラーの φ 完全数と呼ぶ.

$$\varphi(a)=\varphi(P^eq)=\overline{P}P^{e-1}(q-1)=\overline{P}P^{e-1}q-\overline{P}P^{e-1}$$

を P 倍すると

$$P\varphi(a)=\overline{P}P^eq-\overline{P}P^e=\overline{P}a-\overline{P}P^e.$$

$$P\varphi(a)-\overline{P}a=-\overline{P}P^e.$$

一方 $q=\varphi(P^e)+1+m=\overline{P}P^{e-1}+1+m$ を P 倍すると

$$Pq=\overline{P}P^e+P+Pm.$$

$\overline{P}P^e=Pq-Pm-P$ を代入すると

$$P\varphi(a)-\overline{P}a=Pm-Pq+P.$$

$\mathrm{Maxp}(a)$ を a　の最大素因子とするとき, オイラーの φ 完全数 についての方程式は次のとおり:

$$P\varphi(a)=\overline{P}a+Pm-P\overline{\mathrm{Maxp}(a)}$$

これをオイラーの φ 完全数 についての方程式と言う.

オイラーの φ 完全数 の解 a ををを m だけ平行移動した (広義の) をオイラーの φ 完全数という.

5.1 $P = 2, m = -2$

もっとも簡単な $P = 2.m = -2$ の場合を計算してみる.

表 2: $P = 2, m = -2$

a	素因数分解
24	$2^3 * 3$
112	$2^4 * 7$
1984	$2^6 * 31$
32512	$2^8 * 127$
134201344	$2^{14} * 8191$
34359476224	$2^{18} * 131071$
549754765312	$2^{20} * 524287$
9223372032559808512	$2^{32} * 2147483647$

$q = \varphi(P^e) + 1 = 2^{e-1} + 1 - 2 = 2^{e-1} - 1$ が素数という条件なので, q はメルセンヌ素数であり, ここでの $a = 2^e q$ はおしなべて, 完全数の 4 倍である.

オイラー φ 完全数を定義したがまともなものが出てきた.

5.2 $P = 2, m = 0$

次に $m = 0$ の場合を計算する.

表 3: $P = 2, m = 0$

a	素因数分解
12	$2^2 * 3$
40	$2^3 * 5$
544	$2^5 * 17$
131584	$2^9 * 257$
8590065664	$2^{17} * 65537$

素数部分は フェルマ素数で驚くには及ばない.

5.3 $P = 2, m = 2$

$q = 2^{e-1} + 3$ が素数. ここの素数は数が比較的多いことが知られている.

表 4: $P=2, m=2$

a	素因数分解
20	2^2*5
56	2^3*7
176	2^4*11
608	2^5*19
8576	2^7*67
33536	2^8*131
33579008	$2^{13}*4099$
2147680256	$2^{16}*32771$
8590327808	$2^{17}*65539$
137440526336	$2^{19}*262147$
1441151896864686608	$2^{29}*268435459$
2305843015656144896	$2^{31}*1073741827$

6 φ 完全数の方程式の解

7 微小解

$m=0, e=1$ のとき $P=Maxp(a)$ とおくと $a=Pq(P>q:)$ 素数, は

$$\varphi(a)=\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}$$

の解になることは一般的に証明できる.

実際, $\varphi(a)=\overline{P}\overline{q}$, $\mathrm{Maxp}(a)=P$ によって

$$\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}=\overline{P}q-\overline{P}=\overline{P}\overline{q}=\varphi(a).$$

よって $\varphi(a)=\frac{\overline{P}a}{P}-\overline{\mathrm{Maxp}(a)}$.

$m=0$ のときの解 $a=Pq(P>q:)$ 素数) を微小解という. 微小解は φ 完全数の方程式 $(*)$ に特有の解である.

8 定理と証明

定理 1 $m\geq 0$ のとき

$$P\varphi(a)=\overline{P}a+Pm-P\overline{Maxp(a)}$$

を満たす解は

$\langle 1\rangle$ $m=0, e=1$ のとき微小解 $a=Pq(P>q)$ となる.

$\langle 2 \rangle$ $m = P - 1$ のときの微小解 $a = P^e$.

$\langle 3 \rangle$ $e > 1$ のとき a は $(\varphi, m)-$ 完全数

$\langle 4 \rangle$ $e = 1$ のとき $a = Pq$, $q = P + m$ は素数.

Proof.
a は定義式より P の倍数なので $a = P^e L$　(P, L は互いに素)　と書ける. よって次式を満たす:

$$P\varphi(a) = P^e \overline{P}\varphi(L), \overline{P}a = P^e \overline{P}L.$$

$L = 1$ のとき $a = P^e$, $P\varphi(a) = P^e\overline{P} = \overline{P}a, \mathrm{Maxp}(a) = P$ なので

$$P\varphi(a) = P^e\overline{P}, \overline{P}a + Pm - P\overline{\mathrm{Maxp}(a)} = \overline{P}P^e + Pm - P\overline{P}$$

により $Pm - P\overline{P} = 0$. P で除して,$m = P - 1$.
$m = P - 1$ のとき, $a = P^e$ も微小解という.
$L \geq 2$ のとき $a = P^e L$.
$P\varphi(a) = P^e\overline{P}\varphi(L), \overline{P}a = P^e\overline{P}L$ なので

$$P\varphi(a) - \overline{P}a = -P^e\overline{P}(L - \varphi(L)) = Pm - P\overline{\mathrm{Maxp}(a)}.$$

P で除して

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m.$$

(1) L が素数でないとき.
$L - \varphi(L) \geq \mathrm{Maxp}(L)$ を用いて

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)).$$

(a) $P > \mathrm{Maxp}(L)$ の場合,$\mathrm{Maxp}(a) = P, \mathrm{Maxp}(L) \geq 2$.

$$\overline{P} = P - 1 = \overline{\mathrm{Maxp}(a)} \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)) \geq 2\overline{P}.$$

(b) $P < \mathrm{Maxp}(L)$ の場合,$\mathrm{Maxp}(a) = \mathrm{Maxp}(L) \geq 2$.

$$\overline{\mathrm{Maxp}(L)} = \overline{\mathrm{Maxp}(a)} \geq P^{e-1}\overline{P}(\mathrm{Maxp}(L)) \geq \mathrm{Maxp}(L).$$

かくて矛盾.
(2) L が素数 q のとき.
$m \geq 0$ なので

$$\overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P}(L - \varphi(L)) + m = P^{e-1}\overline{P}(q - \varphi(q)) + m \geq P^{e-1}\overline{P}.$$

$a = P^e q$ なので $\mathrm{Maxp}(a) = P$ または $\mathrm{Maxp}(a) = \mathrm{Maxp}(q) = q$.

(a) $\mathrm{Maxp}(a) = P$ とすると,

$$\overline{P} = \overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P} + m.$$

これより, $e = 1, m = 0, P > q$. $a = Pq$ は微小解.

(b) $\mathrm{Maxp}(a) = q$ とすると,

$$\overline{q} = \overline{\mathrm{Maxp}(a)} = P^{e-1}\overline{P} + m.$$

これより, $q = P^{e-1}\overline{P} + 1 + m$. $e > 1$ のとき a は $(\varphi, m)-$ 完全数.

かくて $e = 1$ のとき $q = P + m$ が素数なら $a = Pq$ は解. これも微小解という. 微小解は形が単純で条件も確かめやすいが, 普通の解に比べもて芸のない解なのである.

このようにして, $m \geq 0$ の場合にはオイラーの φ 完全数の基本問題は解決した.

しかし解決しても困ることがある. 問題がなくなって失業状態になるから.

そこで　$m < 0$ の場合について詳しく調べることにした.

$P = 2$ の場合に限っても興味ある結果がいろいろ出てきて, 思いのほか豊穣の大地が広がっていたのである.

9　$P=2$ のときの広義のオイラー φ 完全数

$P=2$ のとき m だけ平行移動した広義のオイラー φ 完全数を次のように分類した調べる.

I 型. $m \geq 0, m$: 偶数
II 型. $m < 0, m$: 偶数
III 型. $m < 0, m$: 奇数
IV 型. $m \geq 0, m$: 奇数

10　I 型,　$m \geq 0, m$: 偶数

広義のオイラー φ 完全数をもっとも簡単な場合からパソコンで調べよう.

10.1　$P=2, m=0$

広義のオイラー φ 完全数をもっとも簡単な場合からパソコンで調べよう.

表 5: $P=2, m=0$

a	素因数分解
12	$2^2 * 3$
40	$2^3 * 5$
544	$2^5 * 17$
131584	$2^9 * 257$

10.2　$P=2, m=2; m=4$

表 6: $P=2, m=2; m=4$

$m=2$		$m=4$	
a	素因数分解	a	素因数分解
20	$2^2 * 5$	28	$2^2 * 7$
56	$2^3 * 7$	208	$2^4 * 13$
176	$2^4 * 11$	2368	$2^6 * 37$
608	$2^5 * 19$		
8576	$2^7 * 67$		
33536	$2^8 * 131$		

これらの解はすべて $a = 2^e q, q = 2^{e-1} + 1 + m$: 素数の形になっている. これを通常解という.

$m \geq 0$ の場合は, オイラー完全数の基本定理により広義のオイラー φ 完全数は狭義のオイラー φ 完全数になる. パソコンによる結果は基本定理を裏付ける.

11 II 型, $m < 0, m$: 偶数

11.1 $P = 2, m = -2$

表 7: $P = 2, m = -2$

a	素因数分解	$\varphi(a)$
24	$[2^3, 3]$	8
112	$[2^4, 7]$	48
1984	$[2^6, 31]$	960
32512	$[2^8, 127]$	16128

以上の場合は, パソコンによる全数調査の結果. $m = -2; q = 2^{e+1} - 1$: 素数の場合については wxmaxima を用いて, 指数　$e < 21$ について調べると結果はすぐ出る.

表 8: $P = 2, m = -2; q = 2^{e-1} - 1, a = 2^e q$: 素数の場合

e	a	素因数分解	$\varphi(a)$
3	24	$2^3 * 3$	8
4	112	$2^4 * 7$	48
6	1984	$2^6 * 31$	960
8	32512	$2^8 * 127$	16128
14	134201344	$2^{14} * 8191$	67092480
18	34359476224	$2^{18} * 131071$	17179607040
20	549754765312	$2^{20} * 524287$	274876858368

以上からこれらはユークリッドの完全数の 4 倍であることがわかる.

表 9: $P = 2, m = -4$

a	素因数分解	$\varphi(a)$
36	$[2^2, 3^2]$	12
80	$[2^4, 5]$	32
416	$[2^5, 13]$	192
1856	$[2^6, 29]$	896
7808	$[2^7, 61]$	3840

ここでは $a = 2^2 * 3^2$ が解でこれを非通常解という.

表 10: $P = 2, m = -4; q = 2^{e-1} - 3$: 素数の場合

e	a	素因数分解	$\varphi(a)$
3	8	2^3	4
4	80	$2^4 * 5$	32
5	416	$2^5 * 13$	192
6	1856	$2^6 * 29$	896
7	7808	$2^7 * 61$	3840
10	521216	$2^{10} * 509$	260096
11	2091008	$2^{11} * 1021$	1044480
13	33529856	$2^{13} * 4093$	16760832
15	536772608	$2^{15} * 16381$	268369920
21	2199016964096	$2^{21} * 1048573$	1099507433472

$a = 36 = 2^2 * 3^2$ のみが非通常解. それ以外は $a = 2^e q$ とかける解.

表 11: $P = 2, m = -10$

a	素因数分解	$\varphi(a)$
60	$[2^2, 3, 5]$	16
72	$[2^3, 3^2]$	24
224	$[2^5, 7]$	96
1472	$[2^6, 23]$	704

非通常解は　$a = 60 = [2^2, 3, 5]$, $a = 72 = [2^3, 3^2]$.

表 12: $P = 2, m = -10; q = 2^{e-1} - 9$: 素数の場合

e	a	素因数分解	$\varphi(a)$
5	224	$2^5 * 7$	96
6	1472	$2^6 * 23$	704
10	515072	$2^{10} * 503$	257024
12	8351744	$2^{12} * 2039$	4173824
18	34357379072	$2^{18} * 131063$	17178558464

12　II 型のときの証明

$P=2$ のとき方程式は

$$2\varphi(a)=a+2m-2(q-1), q=\mathrm{Maxp}(a)$$

により
$a=2^eL(, L:$ 奇数$), S=-m>0$ とおくとき

$$2^{e-1}\mathrm{co}\varphi(L)=q-1+S.$$

$e>1$ を示すために $e=1$ とする.
S と $q-1$ は偶数なので $\mathrm{co}\varphi(L)$ も偶数.
しかし L は奇数, $\varphi(L)$ は偶数なので $\mathrm{co}\varphi(L)=L-\varphi(L)$ も奇数. これ矛盾した.
かくて $e\geq 2$ が示された.

12.1　$S=2$ のときの証明

まず簡単な場合を扱う.
$S=2$ のとき

$$2^{e-1}\mathrm{co}\varphi(L)=q-1+S=q+1.$$

i). $L:$ 素数なら, $\mathrm{co}\varphi(L)=1$ により ,
$2^{e-1}=1+q$. $q=2^{e-1}-1$. これはメルセンヌ素数. $a=2^eq=4*2^{e-2}q$ これは完全数の 4 倍.

2. $L:$ 非素数なら, $\mathrm{co}\varphi(L)\geq q$ により ,

$$2^e\mathrm{co}\varphi(L)=2(1+q)\geq 2^eq.$$

$(1+q)\geq 2^{e-1}q$ になり矛盾.

12.2　$S=4$ のときの証明

$m=-4$ なので

$$2\varphi(a)=a-6-2q.$$

$a=2^eL, L:$ 奇数, とおくとき

$$2^e\mathrm{co}\varphi(L)=2(3+q).$$

1. $L:$ 素数なら, $\mathrm{co}\varphi(L)=1$ により ,
$2^{e-1}=3+q$. $q=2^{e-1}-3$. これより, $e=4, q=5, a=2^4*5$ など

2. L : 非素数なら, $\mathrm{co}\varphi(L) \geq q$ により ,

$$2^e \mathrm{co}\varphi(L) = 2(3+q) \geq 2^e q.$$

$3+q \geq 2^{e-1}q$ になる. ゆえに
$3 \geq (2^{e-1}-1)q$. $e \geq 2$ のとき $q = 3, e = 2$ になり $a = 2^* 3^2$ のみが解.

13 III 型, $m<0, m$: 偶数

狭義の オイラーの φ 完全数では起こりえない m : 奇数でかつ負の数のときから調査を開始する. 個々の場合にパソコンによる計算で調べてみよう.

$S=-m>0$ とおく. $q=\mathrm{Maxp}(a)$ として a の最大素因子 q を導入すると φ 完全数 についての方程式は

$$2\varphi(a)=a-2S-2(q-1).$$

a は偶数になるので $a=2^eL(\ L:$ 奇数) とおくとき

$$2^{e-1}\mathrm{co}\varphi(L)=S-1+q.$$

S : 奇数なので $S-1+q$ も奇数. よって $e=1; a=2L$.

狭義の オイラーの φ 完全数では $e\geq 2$ が満たされている. S : 奇数という尋常でない場合なので $e=1$ になったと理解しておく.

したがってこの場合 φ 完全数 についての方程式は次のようにごく簡単になる:

$$\mathrm{co}\varphi(L)=S-1+q.$$

13.1 $S=1$

$S=1$ のとき φ 完全数 についての方程式

$$\mathrm{co}\varphi(L)=q$$

を解く.

以前オイラーの余関数を詳しく調べていたので結果は推測できて $L=q^2$ が解. したがって $a=2q^2$.

$2\varphi(a)=a-2q$ なら $a=2q^2$ となる.

この結果は美しい (この証明は後で与える).

13.2 $S=3$ の場合の計算結果

$S=3$ のとき φ 完全数 についての方程式を解く.

$a<1000000$ の範囲でパソコンによる解の全数調査をする.

結果として解が無数にでるがみな $a=6p, (p>3)$ の形をしている. これを通常解という.

表 13: $P=2, S=3$

a	素因数分解
$6p, (p>3)$	$2*3*p$

14　通常解

$S=p$: 奇素数のとき, $p<q$: 奇素数 について $L=pq$ は
$\mathrm{co}\varphi(L)=p+q-1$, $S-1+q=p-1+q$ により $\mathrm{co}\varphi(L)=S-1+q$　を満たす.
$a=2pq$ は次式の解でこれが通常解である.

$$2\varphi(a)=a-2p-2(q-1).$$

このように, $S=p$: 奇素数のとき通常解 $a=2pq$ がある.
$S=p$: 合成数のとき通常解はないが散発的な解はありうる. これらの非通常解を見出すことが興味ある課題である.

14.1　$S=5$ の場合の計算結果

表 14: $P=2, m=-5$

a	素因数分解
$10p,(p>5)$	$2*5*p$

$a=10p,(p>5)$ の形の通常解ばかり出る.

14.2　$S=7$　の場合の計算結果

表 15: $P=2, m=-7$

a	素因数分解
54	$2*3^3$
$14p,(p>7)$	$2*7*p$

通常解 $14p=2*7*p$ 以外に $54=2*3^3$ が最初にでてきた解で, これが非通常解.
非通常解の決定は興味ある問題である.

14.3 $S \geq 11$ の場合の計算結果

S : 奇数 であるが解の無い場合は記さない.

表 16: $P = 2, m < 0$, $S = -m \geq 11$

S	a	素因数分解
11	$22p, (p > 11)$	$2 * 11 * p$
13	$26p, (p > 13)$	$2 * 13 * p$
17	90	$2 * 3^2 * 5$
17	$34p, (p > 19)$	$2 * 17 * p$
21	126	$2 * 3^2 * 7$
21	250	$2 * 5^3$
23	$46p, (p > 23)$	$2 * 23 * p$
29	198	$2 * 3^2 * 11$
29	$58p, (p > 29)$	$2 * 29 * p$
31	64	2^6
31	150	$2 * 3 * 5^2$
31	$62p, (p > 31)$	$2 * 31 * p$
33	234	$2 * 3^2 * 13$
37	$74p, (p > 37)$	$2 * 37 * p$
41	306	$2 * 3^2 * 17$
41	$82p, (p > 41)$	$2 * 41 * p$
43	686	$2 * 7^3$
43	$86p, (p > 43)$	$2 * 43 * p$
45	342	$2 * 3^2 * 19$
47	$94p, (p > 47)$	$2 * 47p$
49	350	$2 * 5^2 * 7$
51	210	$2 * 3 * 5 * 7$
53	414	$2 * 3^2 * 23$
53	$106p, (p > 53)$	$2 * 53 * p$
57	294	$2 * 3 * 7^2$
59	270	$2 * 3^3 * 5$
59	$2 * 118p, (p > 59)$	$2 * 59 * p$

パソコンによる計算の結果, $S = 17$ のとき $a = 2*17*p$ という解以外に $a = 90 = 2*3^2*5$ が出てきた. これは非通常解.

これらの結果から非通常解は最小の通常解より小さいことが推定できる.

S : 非素数なら通常解の大きさはどのように評価できるか

という問題は自然な問いかけである.

15　III 型の場合の証明

以上の結果はパソコンでの計算結果なのでこれから数学的証明を行う.
$S=1$ のとき.

$$\mathrm{co}\varphi(L)=q$$

が方程式でこれを解けばよい. q は L の最大素因子で, L は奇数.

15.1　$S=1$ のときの証明

i) $s(L)=1$.
$L=q^j$ とおくとき, $\mathrm{co}\varphi(L)=q^{j-1}=q$ により $j=2$.
ii) $s(L)\geq 2$.
$L=q^j\mu, (q>\mathrm{Maxp}(\mu))$ と書き, $\mu_0=\mathrm{co}\varphi(\mu)$　とおくとき $\mathrm{co}\varphi(L)=q^{j-1}(\mu+\overline{q}\mu_0=q$
.
これにより $j=1$. $\mu+\overline{q}\mu_0>q$ が成り立つのでこれはおきない.
よって, 奇素数 q に関して $L=q^2$.　よって $a=2q^2$.
$S=3,5$ のときは同様にできるので略し, 非通常解の出る最初の例 $S=7$ を扱う.

15.2　$S=7$　のときの証明

$$\mathrm{co}\varphi(L)=S-1+q=6+q$$

が方程式でこれを解けばよい. q は L の最大素因子で, L は奇数.

$L=q^j, (j\geq 2)$ とおくとき,
$\mathrm{co}\varphi(L)=q^{j-1}=q+6$ によって, $j=3, q^2-q=6$. これより $q=3$. 非通常解 $a=2*3^3$
がでる.

$L=q\mu, q>\mathrm{Maxp}(\varphi(\mu))$ の場合. $\mu_0=\mathrm{co}(\mu)$ とおくとき $\mathrm{co}\varphi(L)=(q-1)\mu_0+\mu$ と
なる.

i) $\mu_0=1$.
$\mathrm{co}\varphi(L)=q+\mu-1$ なので $q+\mu-1=q+6$. よって, $\mu=7$. $q>\mu=7$ が条件で
$a=2*7q=14q$. これは通常解.

μ が非素数なら, μ は奇数なので　1) $\mu_0=3, \mu=9$,2) $\mu_0=5, \mu=25$, 3) $\mu_0=7, \mu=49, 35$ 等.
1) $\mu_0\geq 3, \mu$:非素数のとき, $\mu\geq 9$.

$$\mathrm{co}\varphi(L)\geq 3q+6, \mathrm{co}\varphi(L)=q+6\geq 3q+6.$$

これは不成立.

15.3 $S = 17$ のときの証明

$$\mathrm{co}\varphi(L) = S - 1 + q = 16 + q$$

が方程式

$L = q^j, j \geq 2$ とおくとき,

$\mathrm{co}\varphi(L) = q^{j-1} = q + 16$, によって, $q^{j-1} - q = 16$. これより $j = 3, q(q-1) = 16$. 不成立

i) $\mu_0 = 1$. μ が素数なので

$q + \mu - 1 = q + 16$. よって, $\mu = 17$. $q > \mu = 17$ が条件で $a = 2 * 17q = 34q$. これは通常解.

ii) $\mu_0 > 2$. μ が非素数なので

1) $\mu_0 = 3, \mu = 9$ のとき,

$$\mathrm{co}\varphi(L) = 3q + 6, \mathrm{co}\varphi(L) = q + 16.$$

$3q + 6 = q + 16$ により $2q = 10$. したがって $q = 5, a = 2 * 3^2 * 5$.

16 IV 型 m : 正の奇数

m : 奇数, 負の数 の場合が済んだので m : 奇数, 正の数の場合を扱う. この場合は意外なことにきわめて簡単になる. 小さなツチノコを発見した思いがした.

$P = 2, m = 1, 3, 5, \cdots$

表 17: $P = 2, m = 1, 3, 5, \cdots$

m	$a =$ 素因数分解
1	6=2*3
3	10=2*5
5	14=2*7
9	22=2*11
11	26=2*13
13	none(13+2=15, 非素数)
15	34=2*17
17	38=2*19
19	none(13+2=21, 非素数)
21	46=2*23
23	none((23+2=25, 非素数)

$m + 2 = q$ のとき解は $a = 2q$ のみ
この場合は解が完全に決まるが面白いものはでてこない.
以下証明.
$\mathrm{co}\varphi(L) = q - 1 - m$ を解く.
L が素数なら $\mathrm{co}\varphi(L) = 1 = q - 1 - m$ なので $q = m + 2$.
L が非素数なら $\mathrm{co}\varphi(L) \geq q$ なので $q \leq \mathrm{co}\varphi(L) = q - 1 - m$. 矛盾.