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2期　予稿2改 2016 年3月11日

飯高 茂

平成 28 年 3 月 10 日

1　copm

$s(a) \geq 2$ のとき余関数の値 $\mathrm{co}\varphi(a)$ を下から評価するとき, 平方根ではなくより直接な評価をした方がよい. たとえば, a の最大素因子 $\mathrm{Maxp}(a)$ 用いて下から評価してみよう.

$P = \mathrm{Maxp}(a)$ とおくとき,$a = P^j L$, $P > \mathrm{Maxp}(L)$, と書いてみる.

$\mathrm{copm}(a) = \mathrm{co}\varphi(a) - \mathrm{Maxp}(a)$ と新しい不変量を導入すると

$$\mathrm{copm}(a) = P^{j-1}(L + \overline{P}\rho_0) - P$$

$\mathrm{copm}(a) \leq 51$ の場合をすべて調べる.

1) $j \geq 2$.

下限の評価なので, $j = 2$ のとき計算する.

$$\mathrm{copm}(a) = P(L + \overline{P}\rho_0 - 1).$$

a). $\rho_0 = 1$. すなわち L は素数のとき

$\mathrm{copm}(a) = P(L + \overline{P}\rho_0 - 1) = P(L + P - 2)$.

$P = 3$ のときは $L = 2$ になり $\mathrm{copm}(a) = 9$.

$P = 5$ のときは $L = 3, 2$ になる. それに応じて $\mathrm{copm}(a) = 5(L + 3) = 30, 25$.

$P = 7$ のときは $L = 5, 3, 2$ になる. それに応じて $\mathrm{copm}(a) = 7(L + 5) = 70, 56, 49$.

b). $\rho_0 = 2$. すなわち $L = 4$.

$\mathrm{copm}(a) = P(2P + 1)$. $P = 7, 5, 3$ とすると, それに応じて $\mathrm{copm}(a) = 105, 55, 21$.

$j = 3, P = 3, \rho_0 = 1$. すなわち $a = 3^3 * 2$. すると, $\mathrm{co}\varphi(a) = 3^2 * 2^2 = 36, \mathrm{copm}(a) = 33$

$j = 4, P = 3, \rho_0 = 1$. すなわち $a = 3^4 * 2$. すると, $\mathrm{co}\varphi(a) = 3^3 * 2^2 = 68, \mathrm{copm}(a) = 65$

$j=3, P=5, L=2\rho_0=1$. すなわち $a=5^3*2$. すると, $\mathrm{co}\varphi(a)=5^2*6=150, \mathrm{copm}(a)=145$

2) $j=1$.

a). $\rho_0=1$. すなわち L は素数 P のとき

$L=P, P>P$: となる素数 P について $\mathrm{copm}(a)=P+P-1-P=P-1$. このとき解 $a=PP$ は無数にある.

b). $\rho_0=2$. このとき $L=4$.

$$\mathrm{copm}(a)=2P+2-P=P+2.$$

$P=47,43,41,37,31,23,11,7,5,3$ とすると, それに応じて $\mathrm{copm}(a)=49,45,43,39,33,25,13,9,7,5$.

c). $\rho_0=3$. このとき $L=9$.

$$\mathrm{copm}(a)=3P+6-P=2P+6.$$

$P=23,11,7,5$ とすると, それに応じて $\mathrm{copm}(a)=52,28,20,16$.

d). $\rho_0=4$. このとき $L=8,6$.

$L=8$,

$$\mathrm{copm}(a)=4P+4-P=3P+4.$$

$P=13,11,7,5,3$ とすると, それに応じて $\mathrm{copm}(a)=43,37,25,19,13$.

$L=6$,

$$\mathrm{copm}(a)=4P+2-P=3P+2.$$

$P=17,13,11,7,5$ とすると, それに応じて $\mathrm{copm}(a)=53,41,35,23,17$.

e). $\rho_0=5$. このとき $L=25$.

$$\mathrm{copm}(a)=5P+20-P=4P+20.$$

$P=11,7$ とすると, それに応じて $\mathrm{copm}(a)=64,48$.

f). $\rho_0=6$. このとき $L=10$.

$$\mathrm{copm}(a)=6P+4-P=5P+4.$$

$P=11,7$ とすると, それに応じて $\mathrm{copm}(a)=59,39$.

g). $\rho_0=7$. このとき $L=49, L=15$.

$$\mathrm{copm}(a)=7P+8-P=6P+8.$$

$P=11$ とすると, それに応じて $\mathrm{copm}(a)=108$.

$L=15$. $\rho_0=3+5-1=7$.

$$\mathrm{copm}(a) = 7P + 8 - P = 6P + 8.$$

$P = 7, 11$ に応じて $\mathrm{copm}(a) = 6P + 8 = 50, 74..$

h). $\rho_0 = 8$. このとき $L = 12, 14, 16$.

$$\mathrm{copm}(a) = L + 8P - 8 - P = L + 7P - 8.$$

$L = 12$ とすると,$\mathrm{copm}(a) = 4 + 7P$.
$P = 5$ とすると,$\mathrm{copm}(a) = 39$

$L = 14$ とすると,$\mathrm{copm}(a) = 6 + 7P$.
$P = 11$ とすると,$\mathrm{copm}(a) = 83$

$L = 16$ とすると,$\mathrm{copm}(a) = 8 + 7P$.
$P = 3, 5, 7$ とすると, それに応じて $\mathrm{copm}(a) = 29, 43, 57$.
i). $\rho_0 = 9$. このとき $L = 21, 27$.
$\mathrm{copm}(a) = 8P - 9 + L$.
$L = 21$ とすると, $\mathrm{copm}(a) = 12 + 8P$. $P = 11$ なら $\mathrm{copm}(a) = 100$.
$L = 27$ とすると, $\mathrm{copm}(a) = 27 + 8P$. $P = 5$ なら $\mathrm{copm}(a) = 67$.

$$\mathrm{copm}(a) = L + 8P - 8 - P = L + 7P - 8.$$

j). $\rho_0 \geq 12$ のとき copm が最小になるのは, $P = 3, j = 1, L = 2^e e \geq 5$ になるに違いない.
$\mathrm{copm}(a) = 2^{2+1} - 3 \geq 2^6 - 3 = 64 - 3 = 61$.
以上によると次のパソコンの結果が肯定できる.

表 1: copm その 1

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
6	$[2,3]$	2	2	12	3	1
$2P$	$[2,P]$	–	–	–	–	1
15	$[3,5]$	2	8	24	5	2
$3P$	$[3,P]$	–	–	–	–	2
35	$[5,7]$	2	24	48	7	4
$5P$	$[5,P]$	–	–	–	–	4
12	$[2^2,3]$	2	4	28	3	5
77	$[7,11]$	2	60	96	11	6
$7P$	$[7,P]$	–	–	–	–	6
20	$[2^2,5]$	2	8	42	5	7
18	$[2,3^2]$	2	6	39	3	9
28	$[2^2,7]$	2	12	56	7	9
143	$[11,13]$	2	120	168	13	10
$11P$	$[11,P]$	–	–	–	–	10
221	$[13,17]$	2	192	252	17	12
$13P$	$[13,P]$	–	–	–	–	12

表 2: copm その 2

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
24	$[2^3, 3]$	2	8	60	3	13
44	$[2^2, 11]$	2	20	84	11	13
52	$[2^2, 13]$	2	24	98	13	15
45	$[3^2, 5]$	2	24	78	5	16
323	$[17, 19]$	2	288	360	19	16
$17P$	$[17, P]$	–	–	–	–	16
30	$[2, 3, 5]$	3	8	72	5	17
437	$[19, 23]$	2	396	480	23	18
551	$[19, 29]$	2	504	600	29	18
$19P$	$[19, P]$	–	–	–	–	18
40	$[2^3, 5]$	2	16	90	5	19
68	$[2^2, 17]$	2	32	126	17	19
63	$[3^2, 7]$	2	36	104	7	20
36	$[2^2, 3^2]$	2	12	91	3	21
76	$[2^2, 19]$	2	36	140	19	21
667	$[23, 29]$	2	616	720	29	22
$23P$	$[23, P]$	–	–	–	–	22
50	$[2, 5^2]$	2	20	93	5	25
56	$[2^3, 7]$	2	24	120	7	25
99	$[3^2, 11]$	2	60	156	11	28
899	$[29, 31]$	2	840	960	31	28
$29P$	$[29, P]$	–	–	–	–	28
48	$[2^4, 3]$	2	16	124	3	29

表 3: copm その 3

a	factor	$s(a)$	$\varphi(a)$		Maxp(a)	copm
$31P$	$[31, P]$	$-$	$-$	$-$	$-$	30
116	$[2^2, 29]$	2	56	210	29	31
117	$[3^2, 13]$	2	72	182	13	32
54	$[2, 3^3]$	2	18	120	3	33
124	$[2^2, 31]$	2	60	224	31	33
66	$[2, 3, 11]$	3	20	144	11	35
1517	$[37, 41]$	2	1440	1596	41	36
$37P$	$[37, P]$	$-$	$-$	$-$	$-$	36
88	$[2^3, 11]$	2	40	180	11	37
60	$[2^2, 3, 5]$	3	16	168	5	39
70	$[2, 5, 7]$	3	24	144	7	39
148	$[2^2, 37]$	2	72	266	37	39
153	$[3^2, 17]$	2	96	234	17	40
1763	$[41, 43]$	2	1680	1848	43	40
$41P$	$[41, P]$	$-$	$-$	$-$	$-$	40
78	$[2, 3, 13]$	3	24	168	13	41
80	$[2^4, 5]$	2	32	186	5	43
104	$[2^3, 13]$	2	48	210	13	43
164	$[2^2, 41]$	2	80	294	41	43
171	$[3^2, 19]$	2	108	260	19	44
72	$[2^3, 3^2]$	2	24	195	3	45
172	$[2^2, 43]$	2	84	308	43	45
175	$[5^2, 7]$	2	120	248	7	48
98	$[2, 7^2]$	2	42	171	7	49
188	$[2^2, 47]$	2	92	336	47	49
105	$[3, 5, 7]$	3	48	192	7	50

2 究極の完全数とその平行移動

P を素数とし $\sigma(P^e)$ が素数 q のとき $a = P^e q$ を底が P の **究極の完全数**と呼ぼう．このとき $q = \frac{P^{e+1}-1}{\overline{P}}$ となる．ここで $\overline{P} = P - 1$,$\sigma(a)$: a の約数の和.

究極の完全数を整数 m だけ平行移動する．$q = \frac{P^{e+1}-1}{\overline{P}} + m$ が素数のとき $a = P^e q$ を m だけ平行移動した底が P 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.

(1) を満たすとき

素数 $q = \frac{P^{e+1}-1}{\overline{P}} + m$ を基にして $a = P^e q$ とかけるか?

という問題を究極の完全数の基本問題と言う.

この問題は反例が多くあるが部分解でも解ければ価値がある.

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オイラー関数を使って類似した概念を定義しよう.

$\varphi(P^e), e > 1$ 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 $a = P^e q$ をもって P を底とする φ **完全数**と定義する.

表 4: $P = 2$ 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

$e > 4$ なら $e \equiv 1 \mod 4; q \equiv 7; a \equiv 4\ ; \varphi(a) \equiv 6 \bmod 10$ が成り立つ.

5 つのフェルマー素数に応じて 5 つの φ 完全数ができた．これらはフェルマー φ 完全数 と呼ぶ方がよい．後で一般化されたオイラー φ 完全数がでてくる.

4 φ 弱完全数

$k > 0$ に関して,$e = 1 + 4k, q_k = 2^{4k} + 1, a_k = 2^e q_k$ とおき,

a_k を 2 を底とする φ 弱完全数 という.

φ 弱完全数 の末尾 1 桁は 4

表 5: 2 を底とする φ 弱完全数, 法を 100

k	e	q_k	a_k
1	5	17	44
2	9	57	84
3	13	97	24
4	17	37	64
5	21	77	4
6	25	17	44
7	29	57	84
8	33	97	24
9	37	37	64

φ 弱完全数 の末尾 2 桁は 44,84,24,64,04 が繰り返される
$q = 2^{4k} + 1$ の末尾 1 桁は 7
$q = 2^{4k} + 1$ の末尾 2 桁は 17,57,97,37,77 が繰り返される

4.1　3 を底とするとき

$$q = 2 * 3^{e-1} + 1, a = 3^e q.$$

表 6: $P = 3$ を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	63	$3^2 * 7$	36
3	513	$3^3 * 19$	324
5	39609	$3^5 * 163$	26244
6	355023	$3^6 * 487$	236196
7	3190833	$3^7 * 1459$	2125764
10	2324581983	$3^{10} * 39367$	1549681956
17	11118121262251209	$3^{17} * 86093443$	7412080755407364
18	100063090585419903	$3^{18} * 258280327$	66708726798666276
31	A	$3^{31} * 411782264189299$	$--$
55	B	$3^{55} * 116299474006080119380780339$	$--$
58	C	$3^{58} * 3140085798164163223281069127$	$--$
61	D	$3^{61} * 84782316550432407028588866403$	$--$
66	E	$3^{66} * 206021029217550749079470945356 87$	$--$

$A = 2543469496512978387591628831 53,$
$B = 2028835148113635805758132900880265803031134378226187 3,$
$C = 147902082297484050239767887249537915756946039093072095 03,$
$D = 107820617994865872624790789771848037132145023757699899380 09.$
$E = 636669967197883491262127134516306911101006058595257340533039423$

- $e \equiv 2 \bmod 4$ のとき $q \equiv 7, a \equiv 3 \bmod 10.$
- $e \equiv 1 \bmod 4$ のとき $q \equiv 3, a \equiv 9 \bmod 10.$
- $e \equiv 3 \bmod 4$ のとき $q \equiv 9, a \equiv 3 \bmod 10.$

Proof.
$e \equiv 2 \bmod 4.$
$e = 4k + 2$ となるので, $q = 2(3^{e-1}) + 1 \equiv 1 + 1 = 2 \bmod 5.$ よって $q \equiv 2 + 5 = 7 \bmod 10.$
$a = 3^e q \equiv -4 \times 7 \equiv 3 \bmod 5.$ a は奇数なので $a \equiv 3 \bmod 10.$

$e \equiv 1 \bmod 4.$
$e = 4k + 1$ となるので, $q = 2(3^{e-1}) + 1 \equiv 2 + 1 = 3 \bmod 5.$ よって $q \equiv 3 \bmod 10.$
$a = 3^e q \equiv 3 \times 3 \equiv -1 \bmod 5.$ a は奇数なので $a \equiv 9 \bmod 10.$

$e \equiv 3 \bmod 4.$

$e = 4k + 3$ となるので, $q = 2(3^{e-1}) + 1 \equiv -2 + 1 = 4 \bmod 5$. よって $q \equiv 9 \bmod 10$.
$a = 3^e q \equiv 2 \times -1 \equiv 3 \bmod 5$. a は奇数なので $a \equiv 3 \bmod 10$.

5　φ 完全数の平行移動

m だけ平行移動した 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 $a=P^e q$ を (P を底とする) m だけ平行移動した 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.

5.1　$[P=2, m=2]$

表 7: $P=2, m=2$

$e \mod 4$	e	a	素因数分解	$\varphi(a)$
2	2	20	$2^2 * 5$	8
3	3	56	$2^3 * 7$	24
0	4	176	$2^4 * 11$	80
1	5	608	$2^5 * 19$	288
3	7	8576	$2^7 * 67$	4224
0	8	33536	$2^8 * 131$	16640
1	13	33579008	$2^{13} * 4099$	16785408
0	16	2147680256	$2^{16} * 32771$	1073807360
1	17	8590327808	$2^{17} * 65539$	$--$
3	19	137440526336	$2^{19} * 262147$	$--$
1	29	144115189686468608	$2^{29} * 268435459$	$--$

6　φ 完全数の平行移動の方程式

$q=\varphi(P^e)+1+m, e>1$ が素数になるとき $a=P^e q$ とすると,

$$\begin{aligned}\varphi(a)=\varphi(P^e q) &= P^{e-1}\overline{P}\overline{q}\\ &= P^e\overline{P}(q-1)/P\\ &= P^e q\overline{P}/P - P^{e-1}\overline{P}\\ &= \overline{P}a/P-(q-1-m).\end{aligned}$$

かくして $\mathrm{Maxp}(a)=q$ に注意し

$$\varphi(a)=\frac{\overline{P}}{P}a-\overline{\mathrm{Maxp}(a)}+m. \tag{2}$$

が得られた. 分母を払った次の式もよく使われる.

$$P\varphi(a) = \overline{P}a - P\overline{\mathrm{Maxp}(a)} + Pm. \tag{3}$$

が得られた.

これが m だけ平行移動した φ 完全数の方程式 $(*)$ である.

φ 完全数の方程式 $(*)$ で定義された数は必ずしも φ 完全数になるわけではない.

φ 完全数においては $q = \varphi(P^e) + 1 + m$ が素数になると仮定されているので $1 + m$ は P で割れない.

φ 完全数の方程式 $(*)$ 自身を扱うとき $1+m$ は P で割れない, などのことにこだわらない. 実際に $m = P - 1$ の場合が重要な結果を与えるのである.

6.1 φ 完全数の方程式 $(*)$ の解

7 微小解

$m=0$ のとき $P=Maxp(a)$ とおくと $a=Pq(P>q)$ 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 $a=Pq(P>q)$ 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

1. $m=0$ のとき微小解 $a=Pq(P>q)$ となる.
2. $m=P-1$ のときの微小解 $a=P^e$.
3. $e>1$ のとき a は $(\varphi,m)-$ 完全数
4. $e=1$ 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 $a=P^eL\quad(P,L$ は互いに素$)\quad$ 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,$m=P-1$.

$L\geq 2$ のとき $a=P^eL$.

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

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

$a = P^e q$ 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.

$e = 1$ のとき $q = P + m, a = Pq$.

このようにして, オイラーの φ 完全数の基本問題は解決した. しかし解決してもまた困る. そこで $P = 2, m = -S, S$:奇素数 に制限して調べてみる.

9 $P = 2, m = -S$: 奇素数

S : 奇素数とする. $S < p$ を満たす素数

をとり

a=2Spとする.これがφ 完全数としてみる.

$$2\varphi(a) - a + 2\mathrm{Maxp}(a) - 1 = 2\overline{S}\overline{p} - 2Sp + 2p - 2$$
$$= 2(2 - p - S) - 2p + 2 = -2S$$

よって
$$2\varphi(a) = a - 2\mathrm{Maxp}(a) - 1 - 2S.$$

逆にこの式を満たすとき, a は偶数. そこでいつものように $a = 2^e L, L$:奇数, とおけば $2^e\varphi(L) = 2^e La - 2\overline{\mathrm{Maxp}(a)} - 2S$ により

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

$e > 1$ とすると, 左辺は偶数. $L > 2$ とすると $\mathrm{Maxp}(L) - 1 + S$ は奇数. よって, $e = 1$.

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

L : 素数なら $co\varphi(L) = 1 = \mathrm{Maxp}(L) - 1 + S$. これは矛盾.

L : 素数でないなら $co\varphi(L) - \mathrm{Maxp}(L) > 0$.

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

新しい不変量 $\mathrm{copm1}(L) = co\varphi(L) - \mathrm{Maxp}(L) + 1$ を新たに導入すると $\mathrm{copm1}(L) = S$ となる.

$copm(a)$ の数表をみながら, この値が素数になるものを抜き出す:

$S = 3$ なら $\mathrm{copm1} = 3$. このとき $L = 3p$ となるので, $a = 6p$; 通常解.

$S = 5$ なら $\mathrm{copm1} = 5$. このとき $L = 5p$ となるので, $a = 10p$. 通常解.

$S = 7$ なら $\mathrm{copm1} = 7$. このとき $L = 3^3, a = 2 \times 3^3$. または $L = 7p$ となるので, $a = 14p$. 通常解.

$S = 11$ なら $\mathrm{copm1} = 11$. このとき $L = 11p$ となるので, $a = 22p$. 通常解.

$S = 13$ なら $\mathrm{copm1} = 13$. このとき $L = 13p$ となるので, $a = 26p$.

$S = 17$ なら $\mathrm{copm1} = 17$. このとき $L = 45 = [3^2, 5], a = 90$ 非通常解. または $L = 17p$ となるので, $a = 34p$. 通常解.

$S = 31$ なら $\mathrm{copm1} = 31$. このとき $L = 75 = [3, 5^2], a = 150$ 非通常解. または $L = 31p$ となるので, $a = 62p$. 通常解

$S = 41$ なら $\mathrm{copm1} = 41$. このとき $L = 343 = [3^2, 17], a = 486$ 非通常解. または $L = 41p$ となるので, $a = 2 * 41p$. 通常解

$S = 43$ なら $\mathrm{copm1} = 43$. このとき $L = 343 = [7^3], a = 486$ 非通常解. または $L = 43p$ となるので, $a = 2 * 43p$. 通常解

10 $P=3, m\neq 0$ のとき

$3\varphi(a)=2a-3\overline{\mathrm{Maxp}(a)}+6.$

10.1 $P=3, m=-3$ のとき

表 8: $m=-3; 3\varphi(a)=2a-3\overline{\mathrm{Maxp}(a)}+6$

a	素因数分解	$\varphi(a)$
3	[3]	2
9	$[3^2]$	6
15	$[3,5]$	8
27	$[3^3]$	18
81	$[3^4]$	54
243	$[3^5]$	162
729	$[3^6]$	486
2187	$[3^7]$	1458
6561	$[3^8]$	4374
19683	$[3^9]$	13122

$3\varphi(a)=2a-3\overline{\mathrm{Maxp}(a)}-6.$

10.2 $P=3, m=-2$ のとき

表 9: $P=3, m=-2$

a	素因数分解	$\varphi(a)$
12	$[2^2,3]$	4
45	$[3^2,5]$	24
459	$[3^3,17]$	288
4293	$[3^4,53]$	2808

11　$P = 5, m \neq 0$ のとき

11.1　$P = 5, m = -2$ のとき

表 10: $P = 5; m = -2$

a	素因数分解	$\varphi(a)$
475	$[5^2, 19]$	360

11.2　$P = 5, m = 2$ のとき

表 11: $[P = 5, m = 2]$

a	素因数分解	$\varphi(a)$
35	$[5, 7]$	24
575	$[5^2, 23]$	440
12875	$[5^3, 103]$	10200

$e \geq 2$ のとき $q \equiv 3 \mod 10$ を満たすであろう.
解に $a = 5^e q$ があると仮定すれば $q = 4 * 5^{e-1} + 3$ を満たす.
$4 * 5^{e-1} + 3$ が素数になる e は無限にあるかが問題となりうる.

表 12: $P = 5, m = 2$

e	a	素因子分解	$\varphi(a)$
1	35	$5 * 7$	24
2	575	$5^2 * 23$	440
3	12875	$5^3 * 103$	10200
4	314375	$5^4 * 503$	251000
5	7821875	$5^5 * 2503$	6255000
6	195359375	$5^6 * 12503$	156275000
11	1907348779296875	$5^{11} * 39062503$	1525878984375000

12　$co\varphi(a) - \mathbf{Maxp}(a)$ の値変化

copm= $co\varphi(a) - \mathrm{Maxp}(a)$, cosm= $co\sigma(a) - \mathrm{Maxp}(a)$ とおく.
$co\varphi(a) - \mathrm{Maxp}(a), co\sigma(a) - \mathrm{Maxp}(a)$ の $s(a) \geq 2$ の場合について, 値の変化を調べた.
これから一般的な結論を導き証明することが課題である.

表 13: copm,cosm の表

a	factor	$s(a)$	$\varphi(a)$	$\sigma(a)$	Maxp(a)	co$\varphi(a)$	coσ	copm	cosm
$2P, P > 2$	$[2, P]$	2	$-$	$-$	$-$	$-$	$-$	1	3
$3P, P > 3$	$[3, P]$	2	$-$	$-$	$-$	$-$	$-$	2	4
$5P, P > 5$	$[5, P]$	2	$-$	$-$	$-$	$-$	$-$	4	6
12	$[2^2, 3]$	2	4	28	3	8	16	5	13
$7P, P > 7$	$[7, P]$	2	$-$	$-$	$-$	$-$	$-$	6	8
20	$[2^2, 5]$	2	8	42	5	12	22	7	17
18	$[2, 3^2]$	2	6	39	3	12	21	9	18
28	$[2^2, 7]$	2	12	56	7	16	28	9	21
$11P, P > 11$	$[11, P]$	2	$-$	$-$	$-$	$-$		10	12

定理 2 *copm*$=$ *co*$\varphi(a) -$ *Maxp*(a), *cosm*$=$ *co*$\sigma(a) -$ *Maxp*(a) とおく.

$s(a) = 1$ のとき. $a = P^e, e \geq 2$ なら *copm*$=$ $P(P^{e-2} - 1)$.
とくに $a = P^2$ なら *copm*$=$ 0.

$s(a) \geq 2$ のとき
copm$\geq$ 1. *copm*$=$ 1 なら $a = 2P, P > 2$.
copm$=$ 2 なら $a = 3P, P > 3$.
copm$>$ 2 なら *copm*$\geq$ 4. *copm*$=$ 4 なら $a = 5P, P > 5$.
copm$>$ 4 なら *copm*$\geq$ 5. *copm*$=$ 5 なら $a = 12$.
copm$>$ 5 なら *copm*$\geq$ 6. *copm*$=$ 6 なら $a = 7P, P > 11$.

copm1$(L) = co\varphi(L) -$ Maxp$(L) + 1$ の値を個々に調べる.
0) $L = Q, Q$: 素数のとき. copm1$(L) = 2 - Q$.
1) $L = PQ, P > Q$: ともに素数のとき. copm1$(L) = Q$.
2) $L = Q^2, Q$: 素数のとき. copm1$(L) = 1$.
3) $L = 4Q, Q > 2$: 素数のとき. copm1$(L) = 2Q + 2$.
copm1$(L) = 2Q + 2 < 51$ なら $Q \leq 23$.
4) $L = 6Q, Q > 3$: 素数のとき. copm1$(L) = 3Q + 3$.
copm1$(L) = 3Q + 3 < 51$ なら $Q \leq 13$.
5) $L = 8Q, Q > 3$: 素数のとき. copm1$(L) = 3Q + 5$.
copm1$(L) = 3Q + 5 < 51$ なら $Q \leq 13$.
6) $L = 2Q^2, Q \geq 3$: 素数のとき. copm1$(L) = Q^2 + 1$.
copm1$(L) = Q^2 + 1 < 51$ なら $Q \leq 7$.
7) $L = 16Q, Q > 3$: 素数のとき. copm1$(L) = 7Q + 9$.
$Q = 3$ なら copm1$(L) = 30$; $Q = 5$ なら copm1$(L) = 44$.
8) $L = 2Q^3, Q \geq 3$: 素数のとき. copm1$(L) = Q^2 - Q + 1$.
$Q = 3$ なら copm1$(L) = 7$; $Q = 5$ なら copm1$(L) = 21$; $Q = 7$ なら copm1$(L) = 43$, .
9) $L = 16Q, Q > 3$: 素数のとき. copm1$(L) = 7Q + 9$.

$Q=3$ なら $\mathrm{copm1}(L)=30$; $Q=5$ なら $\mathrm{copm1}(L)=44$.
10) $L=5^2Q, Q\geq 7$: 素数のとき. $\mathrm{copm1}(L)=4Q+21$.
$Q=3$ なら $\mathrm{copm1}(L)=36$; $Q=5$ なら $\mathrm{copm1}(L)=41$; $Q=7$ なら $\mathrm{copm1}(L)=49$.

13 はじめに

本書は、雑誌「現代数学」に 2013 年 4 月から連載中の「数学の研究をはじめよう」の初期の連載をまとめたものである. その精神は先進的な高校生や一般の数学好きな市民とともに数学の新しい研究を進めていくさまを見せることである.

実際本書の扱う内容はその大部分が新しく始められた数学の研究であり, 忍耐を持って読み進めた読者は数学という奥深く先の見えない世界に引きずり込まれることになる. 漆黒の世界と思っていると突然展望が開け, 振り返ると今までの霧が晴れて思わず息を呑むこともあるであろう.

本書の執筆に当たって想定した読者は 50 年以上昔の著者自身である. 高校生や大学初年級のときこのような本に出合えたら読み進むにつれて深い感動とともに幸せ感に包まれることであろう. ひたすら昔の自分のために書かれた本書は出来上がってみれば, 類のないものとなった.

本書の成立の歴史についてふれる.

2013 年 3 月に大学を定年退職しその翌日から都内のある私立高校に週に 1,2 度行く事になった. 高校生に数学研究の助言をする事を依頼されたからである.

この話を初めて聞いたとき, 半信半疑であった. 入試準備に関係のない数学研究を高校生は熱心にするものだろうか，案じたのである.

数年前から高校生もオリジナルな研究を行うことそして得られた研究成果を学会で発表することを国が推奨しているそうである. こんなことも動機になり数学研究のクラブができ、オイラー関数、置換群の研究、微分方程式をもちいたシミュレーションなどをそれぞれ個別に行い校内や校外で研究発表を活発にしているという.

実際, 現地の高校生と話してみると「完全数に興味がある」「オイラー関数の研究をしている」などと言う. 彼, または彼女たちは数学での研究テーマを持っている. またはいいテーマを持ちたいと思っている.

大学数学の初歩を学習することではない. 自分たちで研究することが彼, または彼女らには楽しいという. 実にすばらしいことである.

私は彼らの期待にこたえる準備をする必要に迫られた. 高校生にとって興味があり, 高校数学で理解できる範囲の新しい数学研究を行い, 高校生が研究できるネタを作ることになった. 引退教授にとってこれは大きなチャレンジである. その結果, 私も成長し新しい数学の研究ができるようになった.

引退教授だから大学の雑用もレポートや試験の採点, 成績データの整理などに時間をとられることはない. 現役のときより研究時間は 2 倍にも 3 倍にもなった.

半信半疑で引き受けた仕事であったが, 案外うまく行った. 高校生の数学研究への意気込みにはすごいものがあり、得られた研究成果は著しいものであった.

2014 年の秋から神田の本屋さんの 7 階で一般の市民向けの数学講義をすることになった. これは埼玉大学の中川さんの薦めによるものである.

数学の研究をしたいという高校生は都内だけも潜在的にはたくさんいるに違いない. そこで,「高校生にも十分わかる新しい数論研究」をテーマに第 2,4 金曜日の夕刻, 2 時間近く講義することにした.

初回は 30 名を超える参加者だったが, ターゲットにした高校生の参加はなかった. しかし, 小学 1 年生の生徒が最前列に座って, 熱心に聴講しまた質問をするのだった.

彼の最初の質問は忘れがたい. 私が, 約数の和のグラフを示し

「このグラフは複雑で一見多価関数に見えますがよく見ると一価関数です.」

と言った. すると, 小学生が手をあげて

「先生, 多価関数てなんですか」

と質問した. これには真実, びっくりした.

このように始まった市民向けの数学講義は 2 ヶ月に 4 回して 2 ヶ月休むというペースで続けるようになった. また高校生の参加者も相次いだが, 数学好きのスーパー小学生はきわめて熱心な受講生であり続けていることに変わりはない.

いかに新しい研究でもそれに基づいて講義し, 印刷物にまとめて成果を発表しないと続かない.

印刷公表の方は, 現代数学社が自ら申し出て引き受けてくれ雑誌連載になった. それをベースに本書が出版されたというわけである.

最後になったが, 意欲ある小学生と高校生諸君, 講義の場所を提供してくれた神田の本屋さん, そして, 何よりも大事な発表の場を提供してくれた現代数学社の皆様に感謝したい.

2016 年 3 月

放送大学東京多摩学習センター学生控え室にて

飯高茂

14　あとがき

本書は、雑誌「現代数学」に連載中の「数学の研究をはじめよう」の連載をまとめたものである. 2016 年 2 月. 26ヶ月分の内容が区切りよくまとまったので, とりあえず組み版を作ってもらった. すると 460 ページを超えた校正刷りが届いた. このまま本にしたら定価が 8000 円前後になりかねない. ターゲットにした高校生が買えなくなる. そこで三巻にしてしかも 3 ヶ月程度をはさんで出版してくれるように依頼した. 巻 1 を購入し 3 ヶ月かかって読んだところで巻 2 がでればすぐに購入するであろう. そして帰納的に巻 3 , 巻 4 と続けて出版され読者が増加していくことを期待したい.

校正にあたって、寺島成紀さんに尽力してもらった. とくに感謝申し上げたい。本書の成立に力を貸してくれた、松島誠氏、宮本憲一氏にも謝辞を述べたい.

2016 年 3 月

飯高茂

15　著者紹介

1942 年千葉県生まれ

1961 年 県立千葉高校を卒業後, 東京大学理科 1 類から理学部数学科に進学

1967 年 東京大学数物系大学院数学専攻修士課程終了

1967 年 東京大学理学部助手, 専任講師、助教授を経て
1985 年 学習院大学理学部教授
2013 年 学習院大学名誉教授
1971-72 年 プリンストン高等研究所研究員
日本数学会彌永賞, 日本学士院賞受賞 (森重文氏、川又雄二郎氏と共同受賞)
理学博士 (代数多様体の D 次元について)
小平次元, 対数的小平次元, 固有双有理幾何, 混合多種数などの研究に従事
日本数学会理事長, 日本数学会監事, 日本数学教育学会理事　などを歴任