フェルマ素数のファミリ　後編
斜陽の系図

飯高 茂

1　はじめに

本章の目的は N が正の奇数の場合に $2\varphi(a)-a=N$ の解の構造を系図を作って説明することにある.

フェルマ素数のファミリというシリーズの題名は研究がまだ進まないうちに決めたものであるが研究の進展に伴って予想外の結果が出て, ついに系図という概念にたどり着いた.

$2\varphi(a)-a=1$　の知られている解の表を載せる.

ここにおいて最初の解 3 に解のコード A1 をつけて, 次の解 3*5 に解のコード A2 をつけこれを続ける.

しかしいささか異質な $a=83623935=3*5*17*353*929$ には コード B1 をつける.　以下同様.

$2\varphi(a)-a=1$　の知られている解の調査ではフェルマ素数でない素数は B1,B2 に現れる 3 つの素数 353,929,83623937 のみである.

表 1: $2\varphi(a)-a=1$　の知られている解

a	素因数分解	解のコード
3	3	A1
15	$3*5$	A2
255	$3*5*17$	A3
65535	$3*5*17*257$	A4
4294967295	3*5*17*257*65537	A5
83623935	$3*5*17*353*929$	B1
6992962672132095	$3*5*17*353*929*83623937$	B2

最初に復習をかねて 3 つの基本概念を説明する.

1.1 第二種転写

補題 1 a は $2\varphi(a)-a=M$ の解とする. 素数 p は a の約数とする.
$a'=ap$ は $2\varphi(a')-a'=pM$ を満たす.

このような $a'=ap$ を第二種転写解という. 第二種転写解以外の解を固有解という.

1.2 無性生殖

補題 2 $2\varphi(a)-a=M$ を満たすとき $a_1=a/M$ と $\mu=N/M$ とがともに整数とする.
$p=a_1+\mu+1$ が素数ならば $a'=ap$ は $2\varphi(a')-a'=N$ を満たす.

このとき無性生殖により $2\varphi(a)-a=M$ の解 a から $2\varphi(a')-a'=N$ の解 a' ができた,(または生まれた) といい記号で $a\longrightarrow a'$ (M,N) と表す.

1.3 有性生殖

$2\varphi(a)-a=M$ の解 a に対して $a<p<q$ となる素数 p,q を用いて $a''=apq$ とおく.

定数 N を $2\varphi(a'')=a''+N$ と定めると $\varphi(a'')=\varphi(a)(p-1)(q-1)$ によって $\Delta=p+q, B=pq$ とおくとき
$a''=aB, 2\varphi(a'')=aB+N$ なので

$$2\varphi(a'')=2\varphi(a)(B-\Delta+1)=(a+M)(B-\Delta+1)=a''+N=aB+N.$$

それゆえ $(a+M)(B-\Delta+1)=aB+N$. そこで

$$\begin{aligned}(a+M)(B-\Delta+1)-aB&=(a+M)(B-\Delta+1)-aB\\&=a(B-\Delta+1)-aB+M(B-\Delta+1)\\&=a(-\Delta+1)+MB-M\Delta+M.\end{aligned}$$

$(a+M)(B-\Delta+1)=aB+N$ なので

$$a(-\Delta+1)+MB-M\Delta+M=N.$$

さて $N=M\mu, a=a_1M$ と整数 μ,a_1 を用いて書けるとする. 上式で M を払うと,

$$a_1(-\Delta+1)+B-\Delta+1=\mu$$

となり整理すると $\widetilde{a_1} = a_1 + 1$ を用いて

$$B - (a_1 + 1)\Delta + a_1 + 1 = \mu.$$

$B - \widetilde{a_1}\Delta + \widetilde{a_1} = \mu$ により $B - \widetilde{a_1}\Delta = \mu - \widetilde{a_1}$ となる.

一方, $p_0 = p - \widetilde{a_1}, p_0 = p - \widetilde{a_1}, B_0 = p_0 q_0$ とおくとき $B_0 = p_0 q_0 = B - \widetilde{a_1}\Delta + \widetilde{a_1}^2$ を満たすので

$$B_0 = \mu - \widetilde{a_1} + \widetilde{a_1}^2.$$

$D = \mu - \widetilde{a_1} + \widetilde{a_1}^2$ とおけば $p_0 q_0 = D$.

ここで, 与えられた $a, \mu, N = M\mu, a = a_1 M$ に対して $D = \mu - \widetilde{a_1} + \widetilde{a_1}^2$ とおき, $p_0 q_0 = D$ と分解するとき $p = p_0 + \widetilde{a}$ と $q = q_0 + \widetilde{a}$ がともに素数となるとすれば, $a'' = apq$ は $2\varphi(a'') - a'' = N$ を満たす.

かくして素数 2 つから N についての解 a'' が誕生したので $a'' = apq$ を有性生殖解という.

次の形にまとめておく.

補題 3 整数 μ, a_1 を用いて $N = M\mu, a = a_1 M$ と書けるとき $\widetilde{a_1} = a_1 + 1$, $D = \mu - \widetilde{a_1} + \widetilde{a_1}^2$ とおく.

$p_0 q_0 = D$ と D を分解し $p = p_0 + \widetilde{a}$ と $q = q_0 + \widetilde{a}$ がともに素数ならば,

$a'' = apq$ は $2\varphi(a'') - a'' = N$ を満たす.

有性生殖により新しい解を探すことができる.

2　$2\varphi(a)-a=1$ の解の系図

$2\varphi(a)-a=1$　の知られている解についての表に戻ると

$A1 \longrightarrow A2 \longrightarrow A3 \longrightarrow A4 \longrightarrow A5, B1 \longrightarrow B2$
および
A3 $\Longrightarrow$ A5,B1.
B1 $\longrightarrow$ B2

これらを $2\varphi(a)-a=1$ の解の系図 (family tree) という.

2.1　斜陽の系図

A3 で有性生殖に成功し A5 と B1　ができた. A5 では無性生殖ができない. B1 では 1 回だけ無性生殖ができる.

このように滅び行く系図がイメージできるのでこれを斜陽の系図と呼ぶ. このようなことが起きるのは次のような素因数分解の事情があるからである.

A3 での有性生殖において, D が素因数分解 $65281 = 97 * 673$ を持ち,$\widetilde{a_1} = 256$ になる. D の 2 因子分解 $D = p_0 q_0$ が 2 通りある.

1) $p_0 = 1, q_0 = 65281$. $p = 257, q = 65537$ はともに素数. $a'' = 4294967295 = 255 * 257 * 65537$ が解. $p = 255 * 257 * 65537 + 2$ は素数ではない.

2) $p_0 = 97, q_0 = 673$. $p = 353, q = 929$ はともに素数. $a'' = 83623935 = 255 * 353 * 929$ が解.

$p = a'' = 255 * 257 * 353 * 929 + 2$ は素数. したがって, $a''p$ が無性生殖の解.

これほど絶妙な素因子分解があるのは単なる偶然ではすまされない. 何らかの数学的理由があるに違いない.

$$A1 \longrightarrow A2 \longrightarrow A3 \longrightarrow A4 \longrightarrow A5$$

が成り立つことも著しいことである.

$a_1 = 3 = 2 + 1 = 2^2 - 1$ とおくと,
$p = a_1 + 2 = 5 = 2^2 + 1, a_2 = a_1 p = (2^2 - 1)(2^2 + 1) = 2^4 - 1.$
$p = a_2 + 2 = 17 = 2^4 + 1 = 17, a_3 = a_2 p = (2^4 - 1)(2^4 + 1) = 2^8 - 1.$
$p = a_3 + 2 = 2^8 + 1, a_4 = a_3 p = 2^{16} - 1 = 65535.$
$p = a_4 + 2 = 65537$ は素数 .$a_5 = a_4 p = 2^{32} - 1.$
しかし, $a_5 + 2 = 2^{32} + 1$ は 641*6700417 と分解され素数ではない .(オイラーによる)

3　$2\varphi(a)-a=3$ の解の系図

$2\varphi(a)-a=3$ の解の系図については固有解に限って考える.

表 2: $2\varphi(a)-a=3$, 固有解のみ

a	素因数分解	解の名前
5	5	C1
21	$3*7$	C2
285	$3*5*19$	C3
27645	$3*5*19*97$	C4
4295098365	$3*5*17*257*65539$	C5
72787965	$3*5*17*397*719$	D1
72787965*24262657	$3*5*17*397*719*24262657$	D2

次のように $2\varphi(a)-a=3$ の固有解の系図を得る.

C1,C2 孤立解,
C3 $\longrightarrow$ C4.(M=N=3)
A3 $\Longrightarrow$ C5, D1, $(M=1,N=3)$
D1 $\longrightarrow$ D2.(M=N=3)

A3 $\Longrightarrow$ C5, D1 において, $M=1$ から $N=3$ に解が飛んでいる. これをワタリともいう.

A3 $\Longrightarrow$ C5, D1, $(M=1,N=3)$, D1 $\longrightarrow$ D2 が斜陽の系図 になっている.

$M=1,\mu=3,a=3*5*17$ での有性生殖において, $D=65283$ が素因数分解 $3*47*463$ を持ち,$\widetilde{a_1}=256$. D の 2 因子分解 $D=p_0q_0$ が 2 通りある.

1) $p_0=1,q_0=65283$. $\widetilde{a_1}=256$ により $p=257,q=65539$. よって $a=4295098365=255*257*65539$ が解.

2) $p_0=3,q_0=47*65283.q=q_0+256=19*161503$ は素数ではない. $(p=3+256=259$ 素数)

3) $p_0=47,q_0=3*65283.p=p_0+256=3*101$ は素数ではない. $(p=3+256=259$: 素数)

4) $p_0=3*47,q_0=65283$. $p=397,q=719$ はともに素数で $a=255*397*719=72787965$ は解.

$p=255*397*719/3+2=24262657$ は素数なので 3*5*17*397*719*24262657 は D1 から無性生殖された解 D2.

こうして, D1 $\longrightarrow$ D2 (M=N=3) となり,

A3 $\Longrightarrow$ C5, D1, $(M = 1, N = 3)$,D1 $\longrightarrow$ D2 (M=N=3) は斜陽の系図となった.

これも偶然とは思えない. 他に斜陽の系図があるだろうか.

4 $2\varphi(a) - a = 5$ の解の系図

表 3: $2\varphi(a) - a = 5$ の解

a	素因数分解	解のコード
7	7	
75	$3 * 5^2$	5A2
1275	$3 * 5^2 * 17$	5A3
327675	$3 * 5^2 * 17 * 257$	5A4
21474836475	$3 * 5^2 * 17 * 257 * 65537$	5A5
418119675	$3 * 5^2 * 17 * 353 * 929$	5B1
34964813360660475	$3 * 5^2 * 17 * 353 * 929 * 83623937$	5B2

5A2 $\longrightarrow$ 5A4 $\longrightarrow$ 5A4,5B1 $\longrightarrow$ 5B2

A3 $\Longrightarrow$ 5A5,5B1. (M=1,N=3)

よって, 5A2 が元になって, 無性生殖, 有性生殖でえられた.

以上が $2\varphi(a) - a = 5$ の解の系図でありこれらが全系図になるかもしれない.

しかしこれらは 7 の他はすべて第 2 転写の解であり.$2\varphi(a) - a = 1$ の解から転写されたものである. 意外性がないのが意外である.

5 $2\varphi(a) - a = 7$ の解の系図

表 4: $2\varphi(a) - a = 7$ の解

a	素因数分解	解のコード
33	$3 * 11$	K1
345	$3 * 5 * 23$	K2
67065	$3 * 5 * 17 * 263$	K3
4295360505	$3 * 5 * 17 * 257 * 65543$	K4

これらの解の形から内生解 (N=7 の場合の解から得られた生殖解, それは 7 の倍数) ではあり得ない.

N=1 の場合の解から得られた転写解はある.

$M = 1, N = 7$ のとき, $\mu = 7$. 以下では無性生殖を考える.

$a = 3$ に対して $p = a + \mu + 1 = a + 8 = 11$ は素数なので $a' = ap = 3 * 11$ が $2\varphi(a') - a' = 7$ を満たす.

$a = 15$ に対して $p = a+\mu+1 = a+8 = 23$ は素数なので $a' = ap = 3*5*23 = 345$ が $2\varphi(a') - a' = 7$ を満たす.

$a = 3 * 5 * 17 = 255$ に対して $p = a + \mu + 1 = a + 8 = 263$ は素数なので $a' = ap = 3 * 5 * 17 * 263 = 67065$ が $2\varphi(a') - a' = 7$ を満たす.

$2\varphi(a) - a = 7$ の解の系図は次のようになると思われる.

A1 $\longrightarrow$ K1;A2 $\longrightarrow$ K2;A3 $\longrightarrow$ K3

A2 $\Longrightarrow$ K3,;A3 $\Longrightarrow$ K4

私はこの系図をみて驚愕した. 本家 (N=1 の場合) からの略奪でできた系図に見える.

6 $2\varphi(a) - a = 9$ の解の系図

表 5: $2\varphi(a) - a = 9$ の固有解

a	素因数分解	解のコード
11	11	Q1
39	$3 * 13$	Q2
231	$3 * 7 * 11$	Q3

ここで素数解 11 が出た. これは次の補題から分かるので, 自明な解というべきもので, まともに扱うには及ばない.

補題 4 $2\varphi(a) - a = N$ の解が素数 p なら $p = N + 2$.

Proof

$2\varphi(p) - p = p - 2 = N$ により $p = N + 2$.

1)$M = 1, N = 9, a = 3$ として無性生殖を行う.

$p = a + N + 1 = 13$ なので, 解 $3 * 13$. ゆえに A1 $\longrightarrow$ Q2 (ワタリ)

2)$M = 1, N = 9, a = 15$ として無性生殖を行う.

$p = a + N + 1 = 25$ 素数ではない

3)$M=3, N=9, a=3*7, \mu=3$ として無性生殖を行う.
$a_1=7$ $p=a_1+\mu+1=7+4=11$. $a'=3*7*11$. C1 $\longrightarrow$ Q3 (ワタリ)
4)$M=3, N=9, a=3*7, \mu=3$ として有性生殖を行っても解がない.
5)$M=1, N=9, a=3, \mu=9$ として有性生殖の解 231=3*7*11.
固有解の系図は
A1 $\longrightarrow$ Q2(M=1,N=9),C1 $\longrightarrow$ Q3 (M=3,N=9),A1 $\Longrightarrow$ Q3. (M=1,N=9)

7 $2\varphi(a)-a=27$ の解の系図

表 6: $2\varphi(a)-a=27$ の固有解

a	素因数分解	解のコード
29	29	R1
93	$3*31$	R2
357	$3*7*17$	R3
645	$3*5*43$	R4
72165	$3*5*17*283$	R5
4296671205	$3*5*17*257*65563$	R6

1)$M=1, N=27, a=3$ として無性生殖を行う.
$p=a+N+1=31$ なので, 解 $3*31$. ゆえに A1 $\longrightarrow$ R2 (ワタリ)
2)$M=1, N=27, a=3*5$ として無性生殖を行う.
$p=a+N+1=43$ なので, 解 $3*5*43$. ゆえに A2 $\longrightarrow$ R4 (ワタリ)
3)$M=3, N=27, a=3*7, \mu=9$ として無性生殖を行う.
$a_1=7, p=a_1+\mu+1=17$ なので, 解 $3*7*17$. ゆえに C2 $\longrightarrow$ R3 (ワタリ)
4)$M=1, N=27, a=3*5*17, \mu=27$ として無性生殖を行う.
$p=a+N+1=255+28=283$ は素数なので, 解 $3*5*283$. ゆえに A3 $\longrightarrow$ R5 (ワタリ)
固有解の系図は
A1 $\longrightarrow$ R2 (M=1,N=27);A2 $\longrightarrow$ R4(M=1,N=27); C2 $\longrightarrow$ R3(M=3,N=27) ;
A3 $\longrightarrow$ R5(M=1,N=27)
A1 $\Longrightarrow$ R3,R4 (M=1,N=27) ; A2 $\Longrightarrow$ R5 (M=1,N=27) ; A3 $\Longrightarrow$ R6 (M=1,N=27)

8　$2\varphi(a)-a=81$ の解の系図

表 7: $2\varphi(a)-a=81$ の固有解

a	素因数分解	解のコード
83		S1
1455	$3*5*97$	S2
85935	$3*5*17*337$	S3
2236335	$3*5*29*53*97$	S4
3733935	$3*5*23*79*137$	S5
4300210095	$3*5*17*257*65617$	S6
18446744417306935215	3*5*17*257*65537*4294967377	S7

固有解の系図は

S1,S4,S5 は孤立解

A2 $\longrightarrow$ S2(M=1,N=81); A3 $\longrightarrow$ S3 (M=1,N=81).

A1 $\Longrightarrow$ S2 (M=1,N=81);A2 $\Longrightarrow$ S3(M=1,N=81);

A3 $\Longrightarrow$ S6 (M=1,N=81),A4 $\Longrightarrow$ S7(M=1,N=81)

S7 という巨大な解が得られたことに私は感動した.

フェルマ素数列 3*5*17*257*65537 にさらに素数 4294967377　を掛けると $2\varphi(a)-a=81$ の解になっている.

解 $3*5*17*257*65537*4294967377$ には無性生殖の力が残っているのだろうか.

ついでに $a=18446745113091637005=3*5*17*257*65537*4294967539$ $2\varphi(a)-a=243$ の解になっていることも記しておく.