フェルマ素数のファミリ　中編
系図の作成

飯高 茂

平成 30 年 5 月 6 日

1　はじめに

目的は N が正の奇数の場合に $2\varphi(a) - a = N$ の解 a の全体的な構造を調べることである.

次に $2\varphi(a) - a = 1$　の知られている解の表 (表 1) 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 $15 = 3 * 5$ 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解 $a = 83623935 = 3 * 5 * 17 * 353 * 929$ には コード B1 をつける. 以下同様.

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

1.1　転写の一般方程式

正の奇数 $M, N (M < N)$ が与えられたとき $2\varphi(a) - a = M$ の解 a について $a' = ap$ とおく. (ここで, p は $a < p$ となる素数)

$2\varphi(a')-a'=N$ によって N を定めると

$$2\varphi(a')=2\varphi(a)(p-1)=(a+M)(p-1)=a'-a+pM-M.$$

一方 $2\varphi(a')=a'+N$ ゆえに $a=(p-1)M-N$. すなわち, $(a+N)/M+1$ が素数 p のとき $a'=ap$ を定義すると $2\varphi(a')-a'=N$ となる.

ここで見方を改めて $\mu=N/M, a_1=a/M$ とおきこれら μ と a_1 は整数とする.

さらに $p=(a+N)/M+1=(a_1M+M\mu)/M+1=a_1+\mu+1$ を素数とするならば

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

次の補題の形に整理しておく.

補題 1 正の奇数 $M, N(M<N)$ が与えられたとき $2\varphi(a)-a=M$ を満たすとする.

$\mu=N/M, a_1=a/M$ とおきこれら μ と a_1 は整数とする.

$p=a_1+\mu+1$ が素数ならば $a'=ap$ は

$2\varphi(a')-a'=M\mu=N$ 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 $a'=ap$ ができた, または生まれたといい解のコードを用いた記号で $A1\longrightarrow a'A2;(M,N)$ などとと表す.

とくに, $N=M$ のとき $\mu=1$ であり, $p=a_1+2$ が素数ならば $a'=ap$ とおくとき $2\varphi(a')-a'=N$ を満たす.

1.2 2素数の添加

$2\varphi(a)-a=M$ 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.

$2\varphi(a'')=a''+N$ により N を定めるとき $\varphi(a'')=\varphi(a)(p-1)(q-1)$.

よって $\Delta=p+q, B=pq$ とおくと

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

.

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

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

$(a+M)(B-\Delta+1)=aB+N$, ゆえに

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

さて $N=M\mu, a=a_1M$ と整数 μ, a_1 を用いて書けるとする. 上の式は

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

となり整理すると

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

$\widetilde{a_1}=a_1+1$ とおくと $B-\widetilde{a_1}\Delta+\widetilde{a_1}=\mu$ となるので $B-\widetilde{a_1}\Delta=\mu-\widetilde{a_1}$.

一方, $p_0=p-\widetilde{a_1}, p_0=p-\widetilde{a_1}$ とおくとき $p_0q_0=B-\widetilde{a_1}\Delta+{\widetilde{a_1}}^2$ を満たすので $B-\widetilde{a_1}\Delta=\mu-\widetilde{a_1}$ を代入して

$$p_0q_0=\mu-\widetilde{a_1}+{\widetilde{a_1}}^2.$$

$D=\mu-\widetilde{a_1}+{\widetilde{a_1}}^2$ とおけば $p_0q_0=D$.

以上を踏まえ 与えられた a, μ, M に対して $N=\mu M, a_1=a/M$ について $D=\mu-\widetilde{a_1}+{\widetilde{a_1}}^2$ とおき, $p_0q_0=D$ と分解する.

$p=p_0+\widetilde{a}$ と $q=q_0+\widetilde{a}$ がともに素数とならば, $a''=apq$ は $2\varphi(a'')-a''=N$ を満たす.

素数 2 つを用いて次なる解が誕生したので $a''=apq$ を a からできた有性生殖解という. 以上をまとめて補題にする.

補題 2 整数 μ, a_1 を用いて $N=M\mu, a=a_1M$ と書けるとき $\widetilde{a_1}=a_1+1$, $D=\mu-\widetilde{a_1}+{\widetilde{a_1}}^2$ とおく. $p_0q_0=D$ と分解するとき,

$p=p_0+\widetilde{a}$ と $q=q_0+\widetilde{a}$ がともに素数ならば, $a''=apq$ は $2\varphi(a'')-a''=N$ を満たす.

これを解のコードの記号で $A2 \Longrightarrow A4$; (M,N) などと表す.

1.3 系図の作成

$2\varphi(a)-a=1$ の知られている解 A3 から有性生殖で A5 と B1 が誕生したので解のコードを用いて

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

と表す.

$2\varphi(a)-a=1$ の知られている解について次の流れができる.

(無性生殖の流れ) $A1 \longrightarrow A2 \longrightarrow A3 \longrightarrow A4 \longrightarrow A5, B1 \longrightarrow B2$

(有性生殖の流れ) $A3 \Longrightarrow A5, B1$

これらで作られる 解のコードと矢印の総体を解の系図 (family history) という.

$2\varphi(a)-a=1$ の知られている解についての系図は上の図式で完了しているような気がする. しかし解の決定もままならない状態で証明できない.

2 $2\varphi(a)-a=3$ の解の系図

無性生殖と有性生殖を使うと $2\varphi(a)-a=3$ の解が多く見つかるのでその系図を作ろう.

表 2: $2\varphi(a)-a=3$, 多く集めたもの

a	素因数分解	解のコード
5	5	C1
9	3^2	3A1
21	$3*7$	C2
45	3^2*5	3A2
285	$3*5*19$	C3
765	3^2*5*17	3A3
27645	$3*5*19*97$	C4
196605	$3^2*5*17*257$	3A4
4295098365	$3*5*17*257*65539$	C5
72787965	$3*5*17*397*719$	D1
3*83623935	$3^2*5*17*353*929$	3B1
3*6992962672132095	$3^2*5*17*353*929*83623937$	3B2
72787965*24262657	$3*5*17*397*719*24262657$	D2

ここで 3^2 で割れる解は第 2 転写でできるのでこれらを除いた表を次に作る. 第 2 転写解以外の解を固有解という.

表 3: $2\varphi(a) - a = 3$, 固有解

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

2.1 無性生殖

1) C2(3*7) から, N=M=3,$\mu = 1, a = 3*7, a_1 = 7$ により, $p = 7 + 2 = 9$ を得る. これは素数ではない.

2) C3 $(3*5*19)$ から, N=M=3,$\mu = 1, a = 3*5*19, a_1 = 5*19$ により, $p = 95 + 2 = 97$ を得る. これは素数なので $a'' = 3*5*19*97$. この解のコードは C4. よって, C3 $\longrightarrow$ C4

3) C4 $(3*5*19*97$) から, N=M=3,$\mu = 1, a = 3*5*19*97, a_1 = 5*19*97$ により, $p = 5*19*97 + 2 = 13*709$. これは素数ではない.

2.2 有性生殖

M=1, $N = 3, \mu = 3, a = 3*5*17$ (A3) から有性生殖を行った結果次のようになった.

$a = 3*5*17 = 255, \widetilde{a} = 256, D = 65283 = 3*47*463 = p_0 q_0$.

1) これより $p_0 = 1, q_0 = 65283$. $p = 257, q = 65283 + 256 = 65539$. 解 $3*5*17*257*65539$. コードは C5.

2) これより $p_0 = 141 = 3*47, q_0 = 463$. $p = 397, q = 463 + 256 = 929$. 解 $3*5*17*397*719$. コードは D1.

ここで $A3 \Longrightarrow C5, D1(M = 1, N = 3)$ が有性生殖による系図である.

$p = 24262657 = 5*17*397*719 + 2$ は素数なので, 無性生殖による解 $a = 3*5*17*397*719*24262657$ が得られた. この解のコードは D2.

かくて次のように $2\varphi(a) - a = 3$ の固有解の系図が得られる.

C1,C2 孤立解,
C3 $\longrightarrow$ C4.

A3 $\Longrightarrow$ C5, D1 ; (M=1,N=3)
D1 $\longrightarrow$ D2.

$2\varphi(a) - a = 3$ の固有解についての系図が上の表で尽きているかどうかはわからない. 何となくこれだけだろうとの予感がある.

3　$2\varphi(a)-a=5$ の解の系図

表 4: $2\varphi(a)-a=5$ 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

ここにおいて 5A2,5A3,5A4 は $2\varphi(a)-a=1$ の解 からの第 2 転写解

無性生殖の系図は

5A2 $\longrightarrow$ 5A4 $\longrightarrow$ 5A4

次に性生殖でできた解を考える.

$2\varphi(a)-a=1$ の解から $M=N=5,\mu=1$ として有性生殖でできた解を探す.

3*5*5(コードは 5A2) から $M=N=5,\mu=1$ として有性生殖でできた解は $327675=3*5^2*17*257$(5A4). これは既出.

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

これの無性生殖を行う, $a_1=a/5=3*5*17*353*929$ に対し, $p=a_1+2=83623937$ は素数.

$a''=5a_1*83623937=3*5^2*17*353*929*83623937$ は 無性生殖解でコードは 5B2.

ゆえに, 5B1 $\longrightarrow$ 5B2.

表 5: $2\varphi(a)-a=5$ の 100 万以下の解

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

よって, 系図は

5A2 $\longrightarrow$ 5A3 $\longrightarrow$ 5A4,

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

5B1 $\longrightarrow$ 5B2

これらが $2\varphi(a)-a=5$ の解の系図の全部になるかもしれない. しかしこれらはすべて $2\varphi(a)-a=5$ の解から第 2 転写で得られた解である.

したがって, $2\varphi(a)-a=5$ の解の系図は $2\varphi(a)-a=1$ の解の系図を単に 5 倍してそのままコピーしたもの (第二転写のこと) になっている.

私は, 系図のコピーが素数の世界にもあるのがいかにも不思議なことだ.

4 $2\varphi(a)-a=N$ の解

第 2 種転写の方程式について次の補題が成立する.

補題 3 素数 p に対して $a=p^j\alpha(j>0,p,\alpha:$ 互いに素 $)$ とする.

a は $2\varphi(a)-a=M$ の解として,$N=pM$ とおくと $a'=p^{j+1}\alpha$ は $2\varphi(a')-a'=pM=N$ を満たす.

$a'=p^{j+1}\alpha$ を第 2 種転写解というが意外にも有用である.

次の表には多くの第 2 種転写解がある. 読者におかれては自分で確かめることを推奨する.

表 6: $2\varphi(a) - a = N$ の解の一部

a	素因数分解	a	素因数分解
N =1		$N = 15$	
15	$3 * 5$	17	17
255	$3 * 5 * 17$	25	5^2
65535	$3 * 5 * 17 * 257$	57	$3 * 19$
$N = 3$		225	$3^2 * 5^2$
5	5	273	$3 * 7 * 13$
9	3^2	465	$3 * 5 * 31$
21	$3 * 7$	1425	$3 * 5^2 * 19$
45	$3^2 * 5$	3825	$3^2 * 5^2 * 17$
285	$3 * 5 * 19$	28785	$3 * 5 * 19 * 101$
765	$3^2 * 5 * 17$	69105	$3 * 5 * 17 * 271$
27645	$3 * 5 * 19 * 97$	138225	$3 * 5^2 * 19 * 97$
196605	$3^2 * 5 * 17 * 257$	983025	$3^2 * 5^2 * 17 * 257$
$N = 5$		$N = 17$	
7	7	19	19
75	$3 * 5^2$	4335	$3 * 5 * 17^2$
1275	$3 * 5^2 * 17$	$k = 19$	
327675	$3 * 5^2 * 17 * 257$	69	$3 * 23$
$N = 7$		18285	$3 * 5 * 23 * 53$
33	$3 * 11$	$N = 21$	
345	$3 * 5 * 23$	23	23
67065	$3 * 5 * 17 * 263$	99	$3^2 * 11$
$N = 9$		147	$3 * 7^2$
11	11	555	$3 * 5 * 37$
27	3^3	1035	$3^2 * 5 * 23$
39	$3 * 13$	6699	$3 * 7 * 11 * 29$
63	$3^2 * 7$	29355	$3 * 5 * 19 * 103$
135	$3^3 * 5$	70635	$3 * 5 * 17 * 277$
231	$3 * 7 * 11$	201195	$3^2 * 5 * 17 * 263$
855	$3^2 * 5 * 19$		
2295	$3^3 * 5 * 17$	$N = 25$	
82935	$3^2 * 5 * 19 * 97$	55	$5 * 11$
589815	$3^3 * 5 * 17 * 257$	87	$3 * 29$
$N = 11$		375	$3 * 5^3$
13	13	615	$3 * 5 * 41$
$N = 13$		6375	$3 * 5^3 * 17$
35	$5 * 7$	71655	$3 * 5 * 17 * 281$
51	$3 * 17$		
435	$3 * 5 * 29$		
68595	$3 * 5 * 17 * 269$		