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　資料2
2016 年2月26日

飯高 茂

平成 27 年 12 月 25 日

1　$P = 3$ の場合

$a = 3^e$ のとき $3\varphi(a) - 2a = 0$ を満たす.
逆に $3\varphi(a) - 2a = 0$ を満たすなら a は 3 の累乗になる.

2　平行移動

$3\varphi(a) - 2a = 0$ を平行移動するとどうなるか.
$3\varphi(a) - 2a = 2, 10, 50$ の場合について調べてみよう.

表 1: $3\varphi(a) - 2a = 2$,

a	素因数分解
5	5
35	5*7
1295	5*7*37

表 2: $3\varphi(a) - 2a = 10$,

a	素因数分解
13	13
25	5^2
55	$5 * 11$
175	$5^2 * 7$
715	$5 * 11 * 13$
1435	$5 * 7 * 41$
6475	$5^2 * 7 * 37$
32395	$5 * 11 * 19 * 31$
248395	$5 * 7 * 47 * 151$

表 3: $3\varphi(a) - 2a = 50$,

a	素因数分解
53	53
119	$7 * 17$
125	5^3
155	$5 * 31$
275	$5^2 * 11$
875	$5^3 * 7$
935	$5 * 11 * 17$
2135	$5 * 7 * 61$
3575	$5^2 * 11 * 13$
7175	$5^2 * 7 * 41$
32375	$5^3 * 7 * 37$
106535	$5 * 11 * 13 * 149$
161975	$5^2 * 11 * 19 * 31$
420455	$5 * 7 * 41 * 293$

2.1 $3\varphi(a) - 2a = x$ の数表

表 4: $3\varphi(a) - 2a = x$,

a	素因数分解				
84	$[2^2, 3, 7]$	3	24	$[2^3, 3]$	-96
96	$[2^5, 3]$	2	32	$[2^5]$	-96
172	$[2^2, 43]$	2	84	$[2^2, 3, 7]$	-92
178	$[2, 89]$	2	88	$[2^3, 11]$	-92
165	$[3, 5, 11]$	3	80	$[2^4, 5]$	-90
225	$[3^2, 5^2]$	2	120	$[2^3, 3, 5]$	-90
152	$[2^3, 19]$	2	72	$[2^3, 3^2]$	-88
164	$[2^2, 41]$	2	80	$[2^4, 5]$	-88
166	$[2, 83]$	2	82	$[2, 41]$	-86
78	$[2, 3, 13]$	3	24	$[2^3, 3]$	-84
158	$[2, 79]$	2	78	$[2, 3, 13]$	-82
100	$[2^2, 5^2]$	2	40	$[2^3, 5]$	-80
112	$[2^4, 7]$	2	48	$[2^4, 3]$	-80
136	$[2^3, 17]$	2	64	$[2^6]$	-80
148	$[2^2, 37]$	2	72	$[2^3, 3^2]$	-80
507	$[3, 13^2]$	2	312	$[2^3, 3, 13]$	-78
146	$[2, 73]$	2	72	$[2^3, 3^2]$	-76
142	$[2, 71]$	2	70	$[2, 5, 7]$	-74
60	$[2^2, 3, 5]$	3	16	$[2^4]$	-72
66	$[2, 3, 11]$	3	20	$[2^2, 5]$	-72
72	$[2^3, 3^2]$	2	24	$[2^3, 3]$	-72
98	$[2, 7^2]$	2	42	$[2, 3, 7]$	-70
134	$[2, 67]$	2	66	$[2, 3, 11]$	-70

表 5: $3\varphi(a) - 2a = x$,

a	素因数分解				
70	$[2, 5, 7]$	3	24	$[2^3, 3]$	-68
124	$[2^2, 31]$	2	60	$[2^2, 3, 5]$	-68
105	$[3, 5, 7]$	3	48	$[2^4, 3]$	-66
363	$[3, 11^2]$	2	220	$[2^2, 5, 11]$	-66
80	$[2^4, 5]$	2	32	$[2^5]$	-64
104	$[2^3, 13]$	2	48	$[2^4, 3]$	-64
116	$[2^2, 29]$	2	56	$[2^3, 7]$	-64
122	$[2, 61]$	2	60	$[2^2, 3, 5]$	-64
128	$[2^7]$	1	64	$[2^6]$	-64
118	$[2, 59]$	2	58	$[2, 29]$	-62
88	$[2^3, 11]$	2	40	$[2^3, 5]$	-56
106	$[2, 53]$	2	52	$[2^2, 13]$	-56
54	$[2, 3^3]$	2	18	$[2, 3^2]$	-54
$-$	$3^3 * p$	$-$	$-$	$-$	-54
999	$[3^3, 37]$	2	648	$[2^3, 3^4]$	-54
92	$[2^2, 23]$	2	44	$[2^2, 11]$	-52
94	$[2, 47]$	2	46	$[2, 23]$	-50
385	$[5, 7, 11]$	3	240	$[2^4, 3, 5]$	-50
42	$[2, 3, 7]$	3	12	$[2^2, 3]$	-48
48	$[2^4, 3]$	2	16	$[2^4]$	-48
86	$[2, 43]$	2	42	$[2, 3, 7]$	-46
455	$[5, 7, 13]$	3	288	$[2^5, 3^2]$	-46
76	$[2^2, 19]$	2	36	$[2^2, 3^2]$	-44
82	$[2, 41]$	2	40	$[2^3, 5]$	-44
147	$[3, 7^2]$	2	84	$[2^2, 3, 7]$	-42

表 6: $3\varphi(a) - 2a = x$,

a	素因数分解				
50	$[2, 5^2]$	2	20	$[2^2, 5]$	-40
56	$[2^3, 7]$	2	24	$[2^3, 3]$	-40
68	$[2^2, 17]$	2	32	$[2^5]$	-40
74	$[2, 37]$	2	36	$[2^2, 3^2]$	-40
595	$[5, 7, 17]$	3	384	$[2^7, 3]$	-38
30	$[2, 3, 5]$	3	8	$[2^3]$	-36
36	$[2^2, 3^2]$	2	12	$[2^2, 3]$	-36
62	$[2, 31]$	2	30	$[2, 3, 5]$	-34
665	$[5, 7, 19]$	3	432	$[2^4, 3^3]$	-34
40	$[2^3, 5]$	2	16	$[2^4]$	-32
52	$[2^2, 13]$	2	24	$[2^3, 3]$	-32
58	$[2, 29]$	2	28	$[2^2, 7]$	-32
64	$[2^6]$	1	32	$[2^5]$	-32
75	$[3, 5^2]$	2	40	$[2^3, 5]$	-30
44	$[2^2, 11]$	2	20	$[2^2, 5]$	-28
46	$[2, 23]$	2	22	$[2, 11]$	-26
805	$[5, 7, 23]$	3	528	$[2^4, 3, 11]$	-26
24	$[2^3, 3]$	2	8	$[2^3]$	-24
38	$[2, 19]$	2	18	$[2, 3^2]$	-22
28	$[2^2, 7]$	2	12	$[2^2, 3]$	-20
34	$[2, 17]$	2	16	$[2^4]$	-20
18	$[2, 3^2]$	2	6	$[2, 3]$	-18
$-$	$9p$	$-$	$-$	$-$	-18
981	$[3^2, 109]$	2	648	$[2^3, 3^4]$	-18
20	$[2^2, 5]$	2	8	$[2^3]$	-16
26	$[2, 13]$	2	12	$[2^2, 3]$	-16
32	$[2^5]$	1	16	$[2^4]$	-16
22	$[2, 11]$	2	10	$[2, 5]$	-14
12	$[2^2, 3]$	2	4	$[2^2]$	-12
14	$[2, 7]$	2	6	$[2, 3]$	-10
10	$[2, 5]$	2	4	$[2^2]$	-8
16	$[2^4]$	1	8	$[2^3]$	-8

表 7: $3\varphi(a) - 2a = x$,

a	素因数分解				
6	$[2,3]$	2	2	$[2]$	-6
$-$	$3p$	$-$	$-$	$-$	-6
993	$[3,331]$	2	660	$[2^2,3,5,11]$	-6
8	$[2^3]$	1	4	$[2^2]$	-4
4	$[2^2]$	1	2	$[2]$	-2
2	$[2]$	1	1	$[1]$	-1
3	$[3]$	1	2	$[2]$	0
$-$	3^e	$-$	$-$	$-$	0
729	$[3^6]$	1	486	$[2,3^5]$	0
5	$[5]$	1	4	$[2^2]$	2
35	$[5,7]$	2	24	$[2^3,3]$	2
7	$[7]$	1	6	$[2,3]$	4
11	$[11]$	1	10	$[2,5]$	8
13	$[13]$	1	12	$[2^2,3]$	10
25	$[5^2]$	1	20	$[2^2,5]$	10
55	$[5,11]$	2	40	$[2^3,5]$	10
175	$[5^2,7]$	2	120	$[2^3,3,5]$	10
715	$[5,11,13]$	3	480	$[2^5,3,5]$	10

表 8: $3\varphi(a) - 2a = x$,

a	素因数分解				
17	$[17]$	1	16	$[2^4]$	14
65	$[5, 13]$	2	48	$[2^4, 3]$	14
245	$[5, 7^2]$	2	168	$[2^3, 3, 7]$	14
19	$[19]$	1	18	$[2, 3^2]$	16
23	$[23]$	1	22	$[2, 11]$	20
85	$[5, 17]$	2	64	$[2^6]$	22
29	$[29]$	1	28	$[2^2, 7]$	26
77	$[7, 11]$	2	60	$[2^2, 3, 5]$	26
95	$[5, 19]$	2	72	$[2^3, 3^2]$	26
31	$[31]$	1	30	$[2, 3, 5]$	28
49	$[7^2]$	1	42	$[2, 3, 7]$	28
37	$[37]$	1	36	$[2^2, 3^2]$	34
91	$[7, 13]$	2	72	$[2^3, 3^2]$	34
115	$[5, 23]$	2	88	$[2^3, 11]$	34
41	$[41]$	1	40	$[2^3, 5]$	38
43	$[43]$	1	42	$[2, 3, 7]$	40
47	$[47]$	1	46	$[2, 23]$	44
145	$[5, 29]$	2	112	$[2^4, 7]$	46
53	$[53]$	1	52	$[2^2, 13]$	50
119	$[7, 17]$	2	96	$[2^5, 3]$	50
125	$[5^3]$	1	100	$[2^2, 5^2]$	50
155	$[5, 31]$	2	120	$[2^3, 3, 5]$	50
275	$[5^2, 11]$	2	200	$[2^3, 5^2]$	50
875	$[5^3, 7]$	2	600	$[2^3, 3, 5^2]$	50
935	$[5, 11, 17]$	3	640	$[2^7, 5]$	50

3 $P = 3, N = -2^\varepsilon$

以上の結果を見ると, 与えられた ε に対して $P = 3, N = -2^\varepsilon$ の解は特色がありそうである.

$N = -8 = -2^3$ で登場した $a = 2 * 5$ は $N = -16 = -2^4$ で $a = 2^2 * 5$ として成長する.

$a = 2^e p$ として出てくる素数は $5, 13, 29, 61, \cdots$ となり無限に続く.

表 9: $3\varphi(a) - 2a = 2^{\varepsilon}$　の解,

a	素因数分解				
80	$[2^4, 5]$	2	32	$[2^5]$	-64
104	$[2^3, 13]$	2	48	$[2^4, 3]$	-64
116	$[2^2, 29]$	2	56	$[2^3, 7]$	-64
122	$[2, 61]$	2	60	$[2^2, 3, 5]$	-64
128	$[2^7]$	1	64	$[2^6]$	-64
40	$[2^3, 5]$	2	16	$[2^4]$	-32
52	$[2^2, 13]$	2	24	$[2^3, 3]$	-32
58	$[2, 29]$	2	28	$[2^2, 7]$	-32
64	$[2^6]$	1	32	$[2^5]$	-32
20	$[2^2, 5]$	2	8	$[2^3]$	-16
26	$[2, 13]$	2	12	$[2^2, 3]$	-16
32	$[2^5]$	1	16	$[2^4]$	-16
10	$[2, 5]$	2	4	$[2^2]$	-8
16	$[2^4]$	1	8	$[2^3]$	-8
8	$[2^3]$	1	4	$[2^2]$	-4
4	$[2^2]$	1	2	$[2]$	-2
2	$[2]$	1	1	$[1]$	-1

3.1　$N = -2^7, -2^8, \cdots - 2^{18}$

表 10: $P = 3, N = -2^7$,

a	素因数分解
154	$2 * 7 * 11$
160	$2^5 * 5$
208	$2^4 * 13$
232	$2^3 * 29$
244	$2^2 * 61$
256	2^8

$N = -2^7$ では 3 素因子を持つ例 $a = 164 = 2 * 7 * 11$ が初めて登場する.

表 11: $P = 3, N = -2^8$,

a	素因数分解
308	$2^2 * 7 * 11$
320	$2^6 * 5$
416	$2^5 * 13$
464	$2^4 * 29$
488	$2^3 * 61$
512	2^9

表 12: $P = 3, N = -2^9$,

a	素因数分解
616	$2^3 * 7 * 11$
640	$2^7 * 5$
832	$2^6 * 13$
928	$2^5 * 29$
976	$2^4 * 61$
1018	$2 * 509$
1024	2^{10}

表 13: $P = 3, N = -2^{10}$,

a	素因数分解
1232	$2^4 * 7 * 11$
1280	$2^8 * 5$
1562	$2 * 11 * 71$
1664	$2^7 * 13$
1856	$2^6 * 29$
1952	$2^5 * 61$
2036	$2^2 * 509$
2042	$2 * 1021$
2048	2^{11}

$N = -2^{10}$ では 3 素因子を持つ新しい例 $a = 1562 = 2 * 11 * 71$ が登場する.

表 14: $P = 3, N = -2^{11}$,

a	素因数分解
2464	$2^5 * 7 * 11$
2560	$2^9 * 5$
3124	$2^2 * 11 * 71$
3328	$2^8 * 13$
3712	$2^7 * 29$
3904	$2^6 * 61$
4072	$2^3 * 509$
4084	$2^2 * 1021$
4096	2^{12}

表 15: $P = 3, N = -2^{12}$,

a	素因数分解
4928	$2^6 * 7 * 11$
5120	$2^{10} * 5$
6248	$2^3 * 11 * 71$
6656	$2^9 * 13$
7424	$2^8 * 29$
7808	$2^7 * 61$
8144	$2^4 * 509$
8168	$2^3 * 1021$
8186	$2 * 4093$
8192	2^{13}

表 16: $P = 3, N = -2^{13}$,

a	素因数分解
9856	$2^7 * 7 * 11$
10240	$2^{11} * 5$
12496	$2^4 * 11 * 71$
13312	$2^{10} * 13$
14848	$2^9 * 29$
15616	$2^8 * 61$
16288	$2^5 * 509$
16336	$2^4 * 1021$
16372	$2^2 * 4093$
16384	2^{14}

表 17: $P = 3, N = -2^{14}$,

a	素因数分解
19712	$2^8 * 7 * 11$
20480	$2^{12} * 5$
24992	$2^5 * 11 * 71$
26624	$2^{11} * 13$
29696	$2^{10} * 29$
31232	$2^9 * 61$
32576	$2^6 * 509$
32672	$2^5 * 1021$
32744	$2^3 * 4093$
32762	$2 * 16381$
32768	2^{15}

表 18: $P = 3, N = -2^{15}$,

a	素因数分解
39424	$2^9 * 7 * 11$
40960	$2^{13} * 5$
49984	$2^6 * 11 * 71$
53248	$2^{12} * 13$
56506	$2 * 19 * 1487$
59392	$2^{11} * 29$
62464	$2^{10} * 61$
65152	$2^7 * 509$
65344	$2^6 * 1021$
65488	$2^4 * 4093$
65524	$2^2 * 16381$
65536	2^{16}

$N = -2^{15}$ では 3 素因子を持つ例 $a = 56506 = 2 * 19 * 1487$ が登場するけれどこの素数の組 19, 1487 は面構えがいい.2 つの素数が離れがたいカップルとなっていることにロマンを感じる.

表 19: $P = 3, N = -2^{16}$,

a	$(a) =$ 素因数分解
78848	$(78848) = 2^{10} * 7 * 11$
81920	$(81920) = 2^{14} * 5$
99968	$(99968) = 2^7 * 11 * 71$
102938	$(102938) = 2 * 11 * 4679$
106496	$(106496) = 2^{13} * 13$
113012	$(113012) = 2^2 * 19 * 1487$
118784	$(118784) = 2^{12} * 29$
124928	$(124928) = 2^{11} * 61$
130304	$(130304) = 2^8 * 509$
130688	$(130688) = 2^7 * 1021$
130976	$(130976) = 2^5 * 4093$
131048	$(131048) = 2^3 * 16381$
131072	$(131072) = 2^{17}$

表 20: $P = 3, N = -2^{17}$,

a	$(a) =$ 素因数分解
157696	$(157696) = 2^{11} * 7 * 11$
163840	$(163840) = 2^{15} * 5$
199936	$(199936) = 2^{8} * 11 * 71$
205876	$(205876) = 2^{2} * 11 * 4679$
212992	$(212992) = 2^{14} * 13$
226024	$(226024) = 2^{3} * 19 * 1487$
237568	$(237568) = 2^{13} * 29$
249856	$(249856) = 2^{12} * 61$
260608	$(260608) = 2^{9} * 509$
261376	$(261376) = 2^{8} * 1021$
261952	$(261952) = 2^{6} * 4093$
262096	$(262096) = 2^{4} * 16381$
262144	$(262144) = 2^{18}$

表 21: $2^{e+1} - 3 = 0$: :素数の場合

e	$2^{e+1} - 3$:素数の場合
2	5
3	13
4	29
5	61
8	509
9	1021
11	4093
13	16381
19	1048573
21	4194301
23	16777213
28	536870909
93	19807040628566084398385987581

表 22: $2^{e+1}-3$, 一般の場合

e	$e \bmod 4$	$2^{e+1}-3$:一般の場合
2	2	$(5) = 5$
3	3	$(13) = 13$
4	0	$(29) = 29$
5	1	$(61) = 61$
6	2	$(125) = 5^3$
7	3	$(253) = 11 * 23$
8	0	$(509) = 509$
9	1	$(1021) = 1021$
10	2	$(2045) = 5 * 409$
11	3	$(4093) = 4093$
12	0	$(8189) = 19 * 431$
13	1	$(16381) = 16381$
14	2	$(32765) = 5 * 6553$
15	3	$(65533) = 13 * 71^2$
16	0	$(131069) = 53 * 2473$
17	1	$(262141) = 11 * 23831$
18	2	$(524285) = 5 * 23 * 47 * 97$
19	3	$(1048573) = 1048573$
20	0	$(2097149) = 773 * 2713$
21	1	$(4194301) = 4194301$
22	2	$(8388605) = 5 * 1677721$
23	3	$(16777213) = 16777213$
24	0	$(33554429) = 479 * 70051$
25	1	$(67108861) = 37 * 349 * 5197$
26	2	$(134217725) = 5^2 * 173 * 31033$
27	3	$(268435453) = 11 * 13 * 1877171$
28	0	$(536870909) = 536870909$
29	1	$(1073741821) = 23 * 46684427$
30	2	$(2147483645) = 5 * 19 * 22605091$

$e \equiv 2 \mod 4$ のとき $Q = 2^{e+1} - 3$ は 5 を素因子に持つ.
$e > 2$ なら Q は合成数.

4 $P = 3, N = -2^{\varepsilon}$

$\varepsilon = 1$ のとき $3\varphi(a) - 2a = -1$.
このとき $a = 2$ のみが解.
Proof. $a > 2$ とすると, $\varphi(a)$ は偶数なので $3\varphi(a) - 2a$ も偶数になり矛盾.
ゆえに, $a = 2$.

やや一般にして a は $3\varphi(a) - 2a = -2^{\varepsilon}$ の解とする.
$\varepsilon \geq 2$ と仮定する.
$3\varphi(a)/2 - a = -2^{\varepsilon-1}$ になる.

1) $\varphi(a)/2$ が奇数ならば, $a = 2p$, または $a = p; (p \equiv 3 \mod 4)$.
$a = 2p$ のとき $3\varphi(2p) = 3p - 3, 2a = 4p$ によって

$$3\varphi(a) - 2a = 3p - 3 - 4p = -3 - p = -2^{\varepsilon}$$

$p \equiv -3 \mod 4$ となり $p \equiv 3 \mod 4$ に矛盾する.
$a = p$ のとき

$$3\varphi(a) - 2a = 3p - 3 - 2p = p - 3 = -2^{\varepsilon}$$

矛盾.

2) $\varphi(a)/2$ が偶数ならば $\varepsilon \geq 2$ を思い出すと, a は偶数.
そこで $a = 2^e L$ とおく.

$$3 * 2^{e-1}\varphi(L) - 4 * L = 2^{e-1}L - 2^{\varepsilon}$$

$\eta = \varepsilon - e + 1$ とおくと,

$$4L - 3\varphi(L) = 2^{\eta}.$$

$L + 3co\varphi(L) = 2^{\eta}$ と書き直せばわかる様に与えられた 2^{η} に対して これを満たす L は有限個である.

1).
L は奇数で各素因子の指数はすべて 1.
2).
$L = p$: 素数と仮定する. $co\varphi(p) = 1$ によって, $p + 3 = 2^{\eta}$ を書き直し $2^{\eta} - 3$ が素数となる η を探す. $p = 2^{\eta} - 3$ とおき $a = 2^e p$ とするとこれが解.
($2^{\eta} - 3$ が素数となるという条件はメルセンヌ素数に類似していてそれを -2 だけ並行移動している)

3).
$L = pq, p < q$ (p, q : 素数) とする.

$$L + 3co\varphi(L) = pq + 3(p + q - 1) = 2^{\eta}$$

を書き直す.$p_0 = p + 3, q_0 = q + 3$ を使うと

$$p_0 q_0 = 12 + 2^{\eta}.$$

```
next_pq(M,A):- D is A^2+A+M,
N is A+1,
euler_univ(N,D).

euler_univ(U1,N):-
write(n=N),nl,
N1 is floor(sqrt(N)+0.1),
for(1=<N1,A),
% write(a=A),put(9),
B is N//A,
AB is A*B,
% write(ab=A*B),put(9),
% write(a=A),
% write(b=B),tab(3),
% write(ab=AB),tab(5),
N =:=AB,
% write(ab=A*B),put(9),

A1 is A+U1,
A1>0,
factorize(A1,Q1),
% write(A1=Q1),
Q1=[X],
B1 is B+U1,
        factorize(B1,R1),
% write(R1),
R1=[Y],
doll_write(pq=X*Y),put(9),
% AAA is X*Y,
% sigma(AAA,SSS),
% write(AAA),put(9),
```

```
% doll_write(a=X*Y),put(9),
% write(s=SSS),
nl,
fail.

euler_univ(U1,N):- !.
```

以下

```
A=-4,M=2^\eta
next_pq(M,A):
```

として $\eta \leq 29$ の範囲で使う.

```
47 ?- next_pq(2^7,-4).
140=[2^2,5,7]
$pq=7*11$
true.

33 ?- next_pq(2^10,-4).
1036=[2^2,7,37]
$pq=11*71$
true.

38 ?- next_pq(2^15,-4).
32780=[2^2,5,11,149]
$pq=19*1487$
true.


39 ?- next_pq(2^16,-4).
65548=[2^2,7,2341]
$pq=11*4679$
true.

42 ?- next_pq(2^19,-4).
524300=[2^2,5^2,7^2,107]
$pq=11*37447$
$pq=67*7487$
$pq=211*2447$
true.
```

```
52 ?- next_pq(2^25,-4).
33554444=[2^2,7,11,108943]
$pq=11*2396743$
true.
```

以上において $p = 11; q = 7, q = 71, q = 4679, q = 37447, q = 2396743$ が目立つ.

5　pを決めて方程式を解く

5.1　$p = 3$

$$L + 3co\varphi(L) = 3q + 3(3 + q - 1) = 2^{\eta}$$

$L = 3q$ も $3co\varphi(L)$ も 3 で割れるが右辺は 2 のべきだから矛盾.

5.2　$p = 5$

$$L + 3co\varphi(L) = 5q + 3(5 + q - 1) = 8q + 12 = 2^{\eta}$$

により,

$$2q + 3 = 2^{\eta - 2}$$

$\eta - 2 > 0$ なら左辺は奇数なので矛盾.
$\eta - 2 = 0$ なら $2q = 2$ なので矛盾.

5.3　$p = 7$

$$L + 3co\varphi(L) = 7q + 3(7 + q - 1) = 10q + 18 = 2^{\eta}$$

ゆえに

$$5q + 9 = 2^{\eta - 1}.$$

よって

$$-1 \equiv 9 \equiv 2^{\eta - 1} \mod 5$$

$2^2 \equiv -1 \mod 5$ によって,

$$1 \equiv 2^{\eta - 3} \mod 5$$

$$\eta \equiv 3 \mod 4$$

$\eta - 1 = 2 + 4k = 6, 10, 14, 18, \cdots$.
次のプログラムを使う:

```
lcophi(A,B,H,Q=QQ):-A0 is 2^H-B,
Q is A0//A,
QP is A0/A,
write(QP),nl,
factorize(Q,QQ).

 ?-  lcophi(5,9,6,K).
11
K = (11=[11]).
```

$q = 11$ は素数なので解 $p = 7, q = 11$ があった.
$5q + 9 = 2^{\eta-1}$ の解は $\eta = 6, q = 11$ のみである.
Proof. $\eta - 1 = 2 + 4K$ によって, 次のように因数分解できる.
$A = 1 + 2K$ とおくとき

$$5q = 2^{\eta-1} - 9 = 2^{2+4K} - 3^2 = (2^A - 3)(2^A + 3)$$

$$2^A - 3 = 2 * 4^K - 3 \equiv 2 * (-1)^K - 3 \mod 5$$

K が 偶数なら

$$2^A + 3 = 2 * 4^K + 3 \equiv 2 * (-1)^2 K + 3 \equiv 0 \mod 5.$$

$q = (2^A - 3)(2^A + 3)/5$ は素数ではない.
K が 奇数なら

$$2^A - 3 = 2 * 4^K - 3 \equiv 2 * (-1)^2 K - 3 \equiv 0 \mod 5.$$

とくに　$K = 1$ のとき $2^3 - 3 = 5$ になり $2^3 + 3 = 11$.
これを除外例とすると $q = (2^A - 3)(2^A + 3)/5$ は素数ではない.

5.4 $p = 11$

$$L + 3co\varphi(L) = 11q + 3(11 + q - 1) = 14q + 30 = 2^{\eta}$$

ゆえに

$$7q + 15 = 2\eta - 1$$

$$1 \equiv 2^{\eta - 1} \mod 7$$

$\eta \equiv 1 \mod 3$ によって,

$$\eta - 1 \equiv 0 \mod 3$$

$\eta - 1 = 3K = 9, 12, 15, 18, 21, 24$

プログラム

```
lcophi(A,B,H,Q=QQ):-A0 is 2^H-B,
Q is A0//A,
QP is A0/A,
write(QP),nl,
factorize(Q,QQ).
```

を次のように使う.

```
1 ?- lcophi(7,15,24,K).
2396743
K = (2396743=[2396743]).
```

$q = 2396743$ は素数なので解.

```
2 ?- lcophi(7,15,21,K).
299591
K = (299591=[17, 17623]).
```

$q = 299591 = 17 * 17623$ は非素数.

```
3 ?- lcophi(7,15,18,K).
37447
K = (37447=[37447]).
```

$q = 37447$ は素数なので解.

```
4 ?- lcophi(7,15,15,K).
4679
K = (4679=[4679]).
```

$q = 4679$ は素数なので解.

```
5 ?- lcophi(7,15,12,K).
583
K = (583=[11, 53]).
```

$q = 583 = 11 * 53$ は非素数.

```
6 ?- lcophi(7,15,9,K).
71
K = (71=[71]).
```

$q = 71$ は素数なので解.
$\eta = 10, q = 71$
$\eta = 16, q = 4679$
$\eta = 19, q = 37447$
$\eta = 25, q = 2396743$
このようにして, q : 素数 の例は無数にありそうである.

5.5 $p = 13$

$$L + 3co\varphi(L) = 13q + 3(13 + q - 1) = 16q + 36 = 2^{\eta}$$

ゆえに

$$4q + 9 = 2^{\eta - 2}$$

矛盾

5.6 $p = 17$

$$L + 3co\varphi(L) = 17q + 3(17 + q - 1) = 20q + 48 = 2^{\eta}$$

ゆえに

$$5q + 12 = 2^{\eta - 2}$$

矛盾

5.7 $p = 19$

$$L + 3co\varphi(L) = 19q + 3(19 + q - 1) = 22q + 54 = 2^{\eta}$$

$$11q + 27 = 2^{\eta - 1}$$

によって,

$$5 \equiv 2^{\eta - 1} \mod 11.$$

$2^4 \equiv 5 \mod 11$ なので

$$1 \equiv 2^{\eta - 5} \mod 11.$$

これより

$$\eta - 5 \equiv 0 \mod 10$$

$\eta - 4 = 4 + 10K$ と書ける.

```
2 ?- lcophi(11,27,14,L).
1487
L = (1487=[1487]).

3 ?- lcophi(11,27,24,L).
1525199
L = (1525199=[13, 23, 5101]).
```

実は解は $q = 1487$ のみ.

5.8 $p = 23$

$$L + 3co\varphi(L) = 23q + 3(23 + q - 1) = 26q + 66 = 2^{\eta}$$

$$13q + 33 = 2^{\eta-1}$$

$33 \equiv 7 \equiv 2^{\eta-1} \bmod 13$

$$7 \quad \equiv \quad 2^1 1 \bmod 13.$$

$2^{\eta-12} \equiv 1 \mod 13$ により

$$\eta - 12 \equiv 0 \mod 12.$$

```
24 ?- lcophi(13,33,11,L).
155
L = (155=[5, 31]).

25 ?- lcophi(13,33,23,L).
645275
L = (645275=[5, 5, 53, 487]).

26 ?- lcophi(13,33,35,L).
2643056795
L = (2643056795=[5, 1783, 296473]).

27 ?- lcophi(13,33,47,L).
10825960642715
L = (10825960642715=[5, 349, 6203988907]).
```

解は発見できない.

5.9 $p = 29$

$$L + 3co\varphi(L) = 29q + 3(29 + q - 1) = 32q + 84 = 2^{\eta}$$

よって

$$8q + 21 = 2^{\eta-3}$$

解はない.

5.10 $p = 31$

$$L + 3co\varphi(L) = 31q + 3(31 + q - 1) = 34q + 90 = 2^{\eta}$$

よって

$$17q + 45 = 2^{\eta-1}$$

$$11 \equiv 2^{\eta-1} \mod 17$$

解はない.

6 生殖と展開

P 奇数を底として、与えられた N について方程式

$$P\varphi(a) - \overline{P}a = N$$

を満たす a を求める問題を考える.

a と互いに素な素数 p をとり, $a' = ap$ が

$$P\varphi(a') - \overline{P}a' = M$$

の解とする.

$\varphi(a') = \varphi(a)(p-1)$ なので

$P\varphi(a)(p-1) - \overline{P}ap = M$, $P\varphi(a) = \overline{P}a + N$ により

$$(p-1)N = M + \overline{P}.$$

この式を満たす, p, M があれば $a' = ap$ は解になるので, 単為生殖による解, とここではよぶ.

$N = \overline{P}, M = \overline{P}M'$ とかける場合が特に有用であり $p = 1 + a + M'$ を満たす.

6.1 有性生殖

$P\varphi(a) - \overline{P}a = N$ の解 a がありこれと互いに素な素数 p, q をとり, $a'' = apq$ が

$$P\varphi(a'') - \overline{P}a'' = M$$

の解とする.

$\varphi(a'') = \varphi(a)\overline{p}\ \overline{q}$, $\Delta = p + q$ とおけば

$$(\overline{P}a+N)(pq-\Delta+1)-\overline{P}apq=M$$

をえる. これより式を変形して

$$Npq-\Delta(\overline{P}a+N)+\overline{P}a=M-N.$$

$N=\overline{P},M=\overline{P}M'$ とかける場合は $\tilde{a}=a+1$ とおくとき

$$pq-\tilde{a}\Delta=M'-a-1.$$

$p_0=p-\tilde{a},q_0=q-\tilde{a}$ とおくとき

$$p_0q_0=M'-a-1+\tilde{a}^2=M'+a^2+a.$$

与えられた $D=M'+a^2+a$ を分解して $D=p_0q_0$ とする. さらに $p=p_0+\tilde{a}.q=q_0+\tilde{a}$ がともに素数になれば $a''=apq$ が解になる. これを有性生殖による解, とここではよぶ.

7 $P=5$

表 23: $P=5,N=4,$

a	素因数分解
119	$7*17$

$a=119=7*17,M'=7,p=a+a+M'=127$:素数. よって解
$P=5,N=28$ の解 $a=15113=7*17*127$ ができる.

7.1 有性生殖による解

$a=119=7*17,M'=7$ について有性生殖により解が 2 個できる.

```
5 ?- next_pq(7,119).
14287=[7,13,157]
$pq=127*2161$
$pq=211*277$
```

これより $P=5, N=4*7=28$ の解
$a=7*17*127*2161$
$a=7*17*211*277$
$P=5, N=4=28$ の第二種転写解として
$a=833=7^2*17$
ができている.

表 24: $P=5, N=28,$

a	素因数分解
143	$11*13$
203	$7*29$
833	7^2*17
6293	$7*29*31$
6923	$7*23*43$
9443	$7*19*71$
15113	$7*17*127$
846713	$7*29*43*97$

表 25: $P = 5, N = 44,$

a	素因数分解
259	$7 * 37$
3289	$11 * 13 * 23$
9709	$7 * 19 * 73$
15589	$7 * 17 * 131$

7.2 $P = 7$ の解の探求

表 26: $P = 7, N = 6,$

a	素因数分解
13	13
209	11*19
44099	11*19*211
1944809999	11*19*211*44101
3782285936099999999	11*19*211*44101* 1944810001

$p = a + 2 = 11 * 19 + 2 = 211$ は素数

$p = a + 2 = 11 * 19 * 211 + 2 = 44101$ は素数

$p = a + 2 = 11 * 19 * 211 * 44101 + 2 = 1944810001$ は素数

$p = a + 2 = 11 * 19 * 211 * 44101 * 1944810001 + 2 = 17 * 222487408005882353$ は 非素数

単為生殖で解が 4 つできている.

有性生殖でも説明できる.

```
7 ?- next_pq(1,209).
43891=[43891]
$pq=211*44101$
true.

8 ?- next_pq(1,209*211).
1944765901=[13,97,109,14149]
$pq=44101*1944810001$
```

8　$P = 11$ の解

表 27: $P = 11, N = 10$,

a	素因数分解
527	17*31
923	13*71
33263	29*31*37
47519	19*41*61

9　$P = 13$ の解

表 28: $P = 13, N = 12$,

a	素因数分解
779	19*41
74359	23*53*61
260831	17*67*229
359839	17*61*347

10　$P = 17$ の解

表 29: $P = 17, N = 16$,

a	素因数分解
1189	29*41
168299	31*61*89
310589	31*43*233
706859	23*73*421

表 30: $P = 23, N = 22,$

a	素因数分解
2759	31*89
344447	53*67*97
399923	47*67*127

11 $P = 23$ の解

以上の解はすべての説明を拒否している.
これらは孤立解として考えざるを得ない.